S. HRG. 98-1266

OVERSIGHT ON COMMUNICATIONS PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON PATENTS, COPYRIGHTS AND TRADEMARKS

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

NINETY-EIGHTH CONGRESS

SECOND SESSION

ON

PRIVACY IN ELECTRONIC COMMUNICATIONS

SEPTEMBER 12, 1984

Serial No. J-98-137

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

40-617 O WASHINGTON : 1985

S521-54

COMMITTEE ON THE JUDICIARY

STROM THURMOND, South Carolina, *Chairman*

CHARLES McC. MATHIAS, JR., Maryland
PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah
ROBERT DOLE, Kansas
ALAN K. SIMPSON, Wyoming
JOHN P. EAST, North Carolina
CHARLES E. GRASSLEY, Iowa
JEREMIAH DENTON, Alabama
ARLEN SPECTER, Pennsylvania

JOSEPH R. BIDEN, JR., Delaware
EDWARD M. KENNEDY, Massachusetts
ROBERT C. BYRD, West Virginia
HOWARD M. METZENBAUM, Ohio
DENNIS DECONCINI, Arizona
PATRICK J. LEAHY, Vermont
MAX BAUCUS, Montana
HOWELL HEFLIN, Alabama

VINTON DEVANE LIDE, *Chief Counsel and Staff Director*
DEBORAH K. OWEN, *General Counsel*
DEBORAH G. BERNSTEIN, *Chief Clerk*
MARK H. GITENSTEIN, *Minority Chief Counsel*

SUBCOMMITTEE ON PATENTS, COPYRIGHTS AND TRADEMARKS

CHARLES McC. MATHIAS, Jr., Maryland, *Chairman*

PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah
ROBERT DOLE, Kansas

HOWARD M. METZENBAUM, Ohio
PATRICK J. LEAHY, Vermont
DENNIS DECONCINI, Arizona

RALPH OMAN, *Chief Counsel*
STEVEN J. METALITZ, *Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
Mathias, Hon. Charles McC., Jr., a U.S. Senator from the State of Maryland, chairman, Subcommittee on Patents, Copyrights and Trademarks	3

CHRONOLOGICAL LIST OF WITNESSES

Caming, H.W. William, attorney, American Telephone & Telegraph Co., accompanied by Dr. Roy P. Weber, American Telephone & Telegraph Co	3
Keeney, John C., Deputy Assistant Attorney General, Criminal Division, Department of Justice, accompanied by Alan Kornblum, Deputy Counsel, Office of Intelligence Policy, Department of Justice	19
Plesser, Ronald L., partner, law firm of Blum, Nash & Railsback, Washington, DC; Stephen Schachman, Bell Atlantic Mobile Systems, Basking Ridge, NJ; and Marvin S. Cohen, on behalf of the Cellular Communications Industry	35

ALPHABETICAL LIST AND MATERIAL SUBMITTED

Caming, H.W. William: Testimony	3
Keeney, John C.:	
Testimony	19
Prepared statement	22
Leahy, Senator Patrick J.:	
Letter to Hon. William French Smith, January 26, 1984	14
Letters from Stephen S. Trott, Assistant Attorney General, Criminal Division, U.S. Department of Justice:	
March 9, 1984	15
June 14, 1984	18
Plesser, Ronald L.:	
Testimony	35
Prepared statement	39
Schachman, Stephen:	
Testimony	45
Prepared statement	46
Weber, Dr. Roy P.: Testimony	5

OVERSIGHT ON COMMUNICATIONS PRIVACY

WEDNESDAY, SEPTEMBER 12, 1984

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
SUBCOMMITTEE ON PATENTS, COPYRIGHTS AND TRADEMARKS,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room SD–226, Dirksen Senate Office Building, Senator Patrick J. Leahy (member of the subcommittee) presiding.

Staff present: Steven J. Metalitz, staff director; Pamela S. Batstone, chief clerk (Subcommittee on Patents, Copyrights and Trademarks); and John Podesta, minority chief counsel (Subcommittee on Security and Terrorism).

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Good morning. I am Patrick Leahy and I first apologize to witnesses for having achieved what I think is a reputation for some would say painful punctuality. I think I have probably ruined all that this morning, and I do apologize.

I think though that we should not lose sight of the fact of how important it is that you are here. I always worry about hearings that come at the end of a congressional session. They are one of two things, either the catchall, unimportant things that somebody does to be able to get out self-serving press release No. 29 of the day, or they are matters that really cannot wait.

I think that the topic today is an issue that really cannot wait. We have talked in the Senate for years about the electronic revolution, the effect on our lives and our sense of privacy. But all we do is talk about it without doing anything about it.

It is clear to me that within a decade our privacy is going to be as rare a commodity as the old hand-cranked telephone. Let me just talk about a problem that grows just as we are sitting here. We have phones ringing all over the country, answer it, and it is not voices you hear but dots and zeros and blips and beeps that come out of it. And that is the information that is going in digit form and this is everything from interbank orders to private, electronic mail hookups.

It is nothing remarkable, but it is remarkable that none of these transmissions are protected from illegal wiretap, because our primary law passed back in 1968 covered only voice transmission; it failed to cover nonaural acquisitions of communications of which computer to computer transmissions are a good example. And I think a lot of people do not even realize that. We send sophisticat-

ed legal documents, a bid, a love letter. It makes no difference what it might be. People assume that—the average person assumes he is protected against wiretapping as they would as if they were on the phone, but as a practical matter they are not. And what happens is a case where technology eats away at what we assume are our protections in the Constitution.

But I do not think that erosion of rights is inevitable. Increasingly information is stored electronically and not on paper, something that we have to realize. Much of that information is maintained not by individuals, but by third-party custodians such as banks and credit card companies and electronic mail services. And communications were once separate and distinct; now they are converging into an interlocking network of broadcast, telephone, and cable communications, all of which can be transmitted in digital form.

In *Olmstead* v. *United States,* back in 1928, the Supreme Court said the fourth amendment did not cover wiretaps because there had been no physical entry into the house or office of the defendant. That was the time when Justice Brandeis dissented and said:

> Time works changes, brings into existence new conditions and purposes. * * * Therefore, the principal in order to be vital must be capable of wider application than the mischief which gave it birth * * * anyone ought to speculate the progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping.
>
> Ways may some day be developed by which the government without removing papers from secret drawers can reproduce them in court and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

It was 1928 when Justice Brandeis said that, and of course, that is precisely the situation we have today.

Now, in 1967 the Supreme Court overruled *Olmstead* and the following year the Congress enacted the Federal wiretape law, but wrote it for aural acquisitions of communications, and they do not cover the situation that we have today.

I think that reform is long overdue. I think that we can develop legislation to cover not only for today but really for any foreseeable technology. And we might have tried to cover every single possible problem, but I think most of us on the committee felt that as time is short—I know that the distinguished chairman of the committee, Senator Mathias, felt this, that with adjournment nearing it made more sense to focus on a specific problem for which an answer might be within our reach this year.

So it would be relatively easy to amend title III to cover the nonaural transmissions, and after reviewing today's testimony I plan to draft an appropriate remedy and introduce it in the Senate, possibly as an amendment to the computer crime bill now pending.

So that is a longer statement than I normally would give, but I wanted to set some kind of an agenda and let you know what we are planning to do. I would also ask that the statement of Senator Mathias, the chairman of the subcommittee, be introduced in the record and also note again my appreciation for Senator Mathias in arranging these hearings and his own recognition of how important this is.

[The prepared statement of Senator Mathias, chairman of the subcommittee, follows:]

PREPARED STATEMENT OF HON. CHARLES MCC. MATHIAS, JR., A U.S. SENATOR FROM THE STATE OF MARYLAND, CHAIRMAN, SUBCOMMITTEE ON PATENTS, COPYRIGHTS AND TRADEMARKS

This morning the Subcommittee on Patents, Copyrights and Trademarks holds an oversight hearing in its jurisdiction over issues affecting the privacy rights of Americans. Our subject today is the privacy of electronic communications. Although no specific legislative proposal is on our agenda, we will explore whether existing law adequately protects the privacy of Americans who, in increasing numbers, are using new forms of electronic communications to talk with one another. At my request, Senator Pat Leahy, who has played a leading role in stimulating interest in this topic, will preside at the hearing.

In the infancy of our Republic, Thomas Jefferson observed that: "laws and institutions must go hand in hand with the progress of the human mind. * * * As new discoveries are made * * * institutions must advance also, and keep pace with the times."

The Subcommittee on Patents, Copyrights and Trademarks has taken Jefferson's admonition to heart. Since its reconstitution at the beginning of the 98th Congress, the subcommittee has tackled several issues that exemplify the challenge of keeping the law up to date with the breakneck pace of technological change. Nowhere is this task more crucial than in the field of communications privacy.

Technological wizardry offers a variety of new communications media—computer-to-computer data transmission, cellular telephone, local area networks, and many more—and individuals and businesses are taking advantage of these new ways to share information of every kind and description.

Some of the messages that these new media carry are highly sensitive. A translation of the digital blips racing by wire, microwave, fibre optics and other paths could reveal proprietary corporate data, or personal medical or financial information. The users of these new networks—and that means all of us—expect legal protection against unwarranted interceptions of this communications stream, whether by overzealous law enforcement officers or private snoops.

But the law as it now stands may not provide that protection. Under the 1968 wiretap law, the privacy of Americans may turn on technical questions—whether or not the communication is carried by wire, whether it is in analog or digital form—that are simply irrelevant to the legitimate expectations of those who transmit and receive information in today's communication networks.

If the law lags behind technology, then our task is to revise the law to catch up. Our witnesses today should give us a good start down that road. Experts from the communications industry will explain the technological context in which these issues arise: a seamless web of communications media that circles the globe as easily as it links one office cubicle to another. Witnesses from the Justice Department and the private bar will outline the legal environment: a regime of protection that depends upon distinctions that today's technology may have rendered archaic. I hope that at the conclusion of this hearing, we will have a better understanding of the changes that are needed to help the legal protection of communications privacy "keep pace with the times."

Senator LEAHY. Our first witness is Mr. William Caming of American Telephone & Telegraph Co., Basking Ridge, NJ, accompanied by Dr. Roy Weber of AT&T. I am always glad to see some part still called AT&T.

Mr. Caming, do you want to start, or Dr. Weber?

STATEMENTS OF H.W. WILLIAM CAMING, ATTORNEY, AMERICAN TELEPHONE & TELEGRAPH CO., ACCOMPANIED BY DR. ROY P. WEBER, AMERICAN TELEPHONE & TELEGRAPH CO.

Mr. CAMING. I am a senior counsel in the corporate headquarters of American Telephone & Telegraph Co. My areas of primary responsibility have since 1965 included, from a legal standpoint, oversight over matters pertaining to privacy, corporate security, and information technology. I wish to thank the subcommittee for the opportunity to present at its request an overview of the explosive impact of technology upon telecommunications.

Even George Orwell could not have foreseen the extraordinary advances in technology that have taken place within the past decade. The confluence of information technologies inextricably linking telecommunications and computers has compressed time and distance and ushered in a new information age. These scientific breakthroughs in turn have blurred the distinction during transmission between voice communications and nonvoice communications such as data.

It will be recalled, as you mentioned, that the wiretapping proscriptions of title III of the Federal Omnibus Crime Control and Safe Streets Act apply solely to the unauthorized interception of voice conversations. The statute expressly limits the term "intercept" to the aural acquisition of the contents of a wire or oral communications through the use of an electronic, mechanical, or other device.

In this regard, I wish to stress the singular importance that AT&T has always placed upon preserving the privacy of its customers' telecommunications. Such privacy is a basic concept in our business. We believe our customers have an inherent right to feel that they can use our facilities, regardless of the form that the telecommunications may take, with the same degree of privacy they enjoy when talking face to face.

Any undermining of this confidence would seriously impair the usefulness and value of telecommunications. Thus, all AT&T operating practices and service offerings fully recognize the imperativeness of protecting such privacy.

Over the years, we have repeatedly endorsed legislation that would make wiretapping as such unlawful. We said we strongly oppose any invasion of the privacy of communications by illegal wiretapping and, accordingly, welcome Federal and State legislation that would comprehensively protect and strengthen such privacy.

As we all know, the dissemination of data, electronic mail, graphics, and other nonvoice communications is ever increasing at an exponential rate and rapidly becoming indistinguishable during transmission from voice communications, as Dr. Weber will show.

Thus, there is a compelling need for Congress to determine whether as a matter of national public policy the reach of Federal law should be extended to prohibit the unlawful interception of all forms of communication whenever there is an expectation of privacy under circumstances that society believes reasonably justify such expectation, regardless of whether the communication is voice or nonvoice, transmitted in analog or digitized format or both, by wire or radio, over cable or satellite. Seemingly, all such forms of communication should enjoy equal protection under the law.

At this juncture, it is a pleasure to introduce Dr. Roy P. Weber, formerly of our Bell Laboratories, and currently division manager of service concepts at AT&T Communications. Dr. Weber has an unusual breadth of experience and expertise in telecommunications network technology, as well as an excellent sense of humor. And he will describe a number of the dramatic advances in technology to which I have just alluded. At the conclusion of his presentation, we shall be pleased to answer any questions that you may have with

respect to the legal or other consequences flowing from these developments.

STATEMENT OF DR. ROY P. WEBER

Dr. WEBER. With the help of some slides, I would like to present a very brief overview of the rapid changes that are occurring in telecommunications in this country today. These changes are in basic technology, how that technology is being applied in the network, and how customers are using the resulting services to solve their business and personal problems.

The key point that I will make, and I think is relevant to this subcommittee, is that the distinction between voice, data, image, and video is rapidly diminishing. What was once a telephone system that carried only voice is rapidly becoming an Integrated Services Digital Network, which carries the four forms of communication: voice, data, video, and image.

Let me suggest an example that is well within the technical state of the art today. Consider a medical doctor in New York who wishes to consult with a specialist in Texas. Assume the doctor in New York has a particular patient's records, including electrocardiogram, chest x ray, and the like, stored in a computer file in New York. The doctor in New York might well call the doctor in Texas, talk to that doctor, and during the conversation transmit the entire patient's records, including the chest x rays, to Texas for immediate consultation.

That particular communication involves both voice, data, and image. I personally believe that in the near future all sorts of forms and combinations of voice, data, video, and image communication will be commonplace. And those are the four forms that I am going to talk about.

Let me highlight the video for a moment. By video, I am referring to teleconferencing kinds of services which have somewhat lower fidelity than commercial TV, which are becoming popular in business situations. And by image I am referring to, for example, this particular slide being transmitted as opposed to a video image.

In today's marketplace, one sees the beginning of telephone sets that are designed to take advantage of such integrated communications. A person using this particular terminal might be talking to somebody and during the conversation might refer to a data file in a distant city to continue the conversation and maybe transmit that data file to the person that he is talking to while they are talking, and that indeed is both voice and data communication transmissions happening simultaneously and is a rather dramatic event in our network.

Let me talk about basic technology for just a moment. Voice is a continuous analog process as is represented on the top of this slide, and the telephone networks were originally designed to transport these continuous voice frequency signals. When computers were introduced, their natural language of sequences of zeros and ones had to be modulated to be made to look like a voice signal and put in analog form in order to be carried over the network.

In the 1960's, technology was at a point where in selective parts of the network it became efficient to represent voice as sequences

of zeros and ones. Today, technology is to the point where the entire network is very rapidly becoming entirely digital.

Senator LEAHY. When you are talking to somebody, your voice is broken down into——

Dr. WEBER. In bits; you are talking by the bit. What you are doing today when you make an average call in this country, part of the voice is transmitted in an analog form, as represented on the top of that chart, and in many places in the network today in our switching machines, and over the wires that the voice is carried on, a process goes on where your voice is digitized and is represented as a string of bits and may go back and forth between analog and digital several times in an average conversation today.

It is my belief that the way technology is going, it will soon be all bits; not in our lifetimes will it be all bits, but it will happen and that is the direction, but today it is a mixture.

Mr. CAMING. If I may add a lay comment, perhaps to make it a little simpler. In transmission, when we speak into a telephone, there is a conversion of the voice into either analog form or digital form so that if you were listening—if you could listen inside the wire, if it is a wire transmission—you would not hear whether it was data or voice; and if it were susceptible of being heard, they would be nothing more than electromechanical and electronic signals.

Senator LEAHY. That really comes of course to the point, because if all you are hearing is digital, not a voice, even though it is a voice transmission, then it would appear that that is not covered by our wiretap law.

Mr. CAMING. Not to confuse or get you more confused, actually——

Senator LEAHY. We do that all the time. If we have to go out and work for a living, we want to know how to do it, some of us being lawyers.

Mr. CAMING. Perhaps I could start out by saying that when we just had analog signals, the ones at the top of this slide, actually if you intercept the analog signal, you are not intercepting voice, even though it is a voice conversation; you are intercepting signals, electromechanical or electronic. Then, those signals must be demodulated, as it is in the telephone industry at the end of the call, back to a level that can be heard by the human ear as sound, and you thus reproduce the speech.

Now, with data, when you capture that on analog, because it goes on analog, you again capture only electronic signals. That is then at the other end demodulated to a level that the computers can recognize and handle it. And that of course, being nonspeech, cannot be heard.

But the point of emphasis is that actually they are both voice and nonvoice communications being transmitted in both analog and digitized format. There is no distinction between analog carrying voice and data and also digitized carrying voice and data. The only distinction is that there are certain characteristics of the digitized voice that make it more attractive to use and permit greater speed, some cost efficiencies and some greater fidelity. But I wanted to stress that one point.

Senator LEAHY. I see. Thank you.

Dr. WEBER. The network's rapid conversion to a digital format is made possible by two major technologies. The first is microelectronics. This technology is used to code; that is, to convert to zeros and ones and to process the digitized voice.

The second technology that is making the network rapidly become digital is fiber optics. These hair thin strands of glass transmit light pulses, the light being pulsed hundreds of millions or billions of times a second, and these pulses, representing zeros and ones, are encodings of thousands of voice, data, or image communications.

Let me now take a global look at the telecommunications network. A recent article in High Technology, I believe, captured the essence of the current modern network. It stated that the telephone system is beginning to look like the world's largest computer. Let me illustrate in cartoon form what this really means, and I will illustrate the types of services that modern computerized telecommunication networks are beginning to offer.

In this example, I have a traveler who on his way to the airport stops at a telephone to change his flight reservations. Instead of getting the altogether too often busy signal or sitting and listening to music in a cue, the caller is asked to enter a telephone number to which a callback is promised within a few minutes. Furthermore, the airline's preferred customers can input a security code and have their calls go to specialized attendants.

Let us now consider the case where a blizzard just struck in one of the cities where the airline has a reservation center. The airline can simply tell the telephone network to automatically take that city out of service and route its intended telephone traffic to another reservations center. The power of the stored-program-controlled network, that one big computer that we have, is being applied to meet the needs of the airline and its customers.

Let us look at a somewhat less complicated example that was introduced a number of years ago that has become very popular with our customers. This service allows credit card users to make a credit card call without the need to talk to an operator. A caller dials zero, the telephone number they are calling, and then, upon being prompted, can put a billing number, a personal identification number into the network.

Senator LEAHY. At which point the computer goes, "Thank you."

Dr. WEBER. Well, one of my problems is, it is always the same accent; and I would like different accents in different parts of the country. In other words, it is a computer saying thank you, and that is an interesting question of whether that is voice or data.

Senator LEAHY. They should be able to speak Pepperidge Farm up in our part of the country.

Dr. WEBER. Nevertheless, it is a very popular, very highly used service, and upon validation the call is then set up and you then talk. And this service architecture, I believe, graphically illustrates the merging of voice communication and data communication that's going on, computer processing, and the use of computer data base files all in the same call; and all that occurs in about a half a second timeframe, what is on that slide.

Pushing technology a bit further, a new networking bridging capability is currently being introduced. A caller from any touchtone

phone in the country will be able to dial a specialized telephone number which instructs the network, using a data base, to find an available port on the so-called network services complex.

The caller can then establish a conference call with up to 59 additional parties. The capability also exists for a parallel data conference to be set up, which is illustrated in red on the slide. This data conference may be used, for instance, to transmit visuals supporting the presentation. So we both have a data conference and a voice conference occurring at the same time with respect to the same material.

Typical conference rooms will then consist of both audio equipment and all sorts of forms of graphic equipment, including electronic blackboards, visual displays, and facsimile devices.

Continuing on my somewhat whirlwind tour of emerging services is the capability of a caller to specifically dial up a high-speed data connection through the public-switched network; in other words, force the call to go through only the digital part of the network and not allow the call to go over any analog facilities. In this emerging service offering, the customer instructs the network to selectively route its call.

The resulting connection will be able to support the transmission of 56,000 bits of information per second. Also, that capability allows alternate voice-data conversations. Sometimes you can have data and sometimes you can have voice over the same connection.

An exciting application of this capability is in high-speed facsimile. At 56,000 bits of information per second that you dialed up through the network, a single page of facts can be sent in the matter of a very few seconds.

Senator LEAHY. Does that mean with a facsimile you can take a sheet of newspaper and do that or is that to reproduce a sheet of something that has been typed out on a typewriter?

Dr. WEBER. No; this is a random piece of paper that you wrote with pencil and it is essentially a processed photograph that is being sent. If you had it in digital form to begin with, you can send it much more rapidly than this.

Senator LEAHY. With all that, you know, you would think someday they would be able to make a speaker phone that would work. [Laughter.]

Dr. WEBER. It depends on whose equipment you buy, I believe. I have one on my desk that works.

Senator LEAHY. See me afterwards; I will negotiate to buy it from you. I have had one for 15 years now and I have yet to get one that works. If anybody starts typing in the other room, you close the door, everything else, one side or the other just gets cut off the conversation entirely. In fact, I have been paying for one now for the last 5 years and I think I have used it three times as a result. Go ahead; I do not mean to interrupt.

The other thing is fascinating. Some of these little prosaic things just somehow fall away.

Dr. WEBER. That is the real world, I guess.

Senator LEAHY. I guess.

Dr. WEBER. Another intriguing application of the switched 56-kilobit service is secure voice. With an all-digital connection that you dialed up, the quality and economics of encrypted voice are im-

proved. And there is an interesting issue—of course, the bits are therefore scrambled. It is an interesting issue of whether that is voice or data being transmitted.

Senator LEAHY. Back on that, secure voice, that is something that has to be done by the parties or is that something that AT&T can do anyway?

Dr. WEBER. No; the intent here is that the caller sets up a 56-kilobit path through the network and purposely instructs the network to selectively route only through certain types of equipment and then the caller does what he wants. They can put facsimile machines at the two ends or they can put scrambling devices at the two ends and it is transparent to the network. We do not know nor do we care.

Mr. CAMING. Just to answer your question, the encryption and decryption is provided by the customer. There are a great many sophisticated forms of it which are readily available commercially, and at least within the Bell system at this time, pardon me, the AT&T system—I have been too long with the Bell system to not be marked with it—we do not offer it as part of the telephone offering.

Senator LEAHY. I was just interested in that a little bit because there is so much going over microwave that it is—so many telephone conversations that it is so easy to pick up, and if you go to downtown Washington and look at where half the antennas on the Soviet embassy are pointing, or out in San Francisco they have set up there on the roof of their consulate out there for eavesdropping. They do it here and they are about to go on to an embassy up on Wisconsin Avenue, the site of which was picked primarily because of its eavesdropping capabilities.

I still find so many of our defense contractors and others who call from the west coast or anywhere else and just do not take advantage of encryption devices; and yet there are encryption devices, especially used in this type of a network, that are untappable. I mean, they are undecipherable except for the machines on either end.

I am just surprised more people do not use these scrambling devices. I hope they, with the ability to use the system better, I hope they start using them.

It is amazing, half the time we do not even use it coming out of the White House where I recall once getting a call from Air Force One; the President does not like using the scrambler phone. It is a little bit hard to hear. So the Signal Corps comes on from the White House first and says, you know, this is going to be an open line. So we use the Secret Service's call name. You do not refer to the President as Mr. President; they call him Rawhide, which is the Secret Service name for him.

Well, you feel kind of silly doing that. You say, and how is Mrs. Rawhide today. Anyway, go ahead.

Dr. WEBER. Another data service that is emerging worldwide is packet transport. Here a host computer creates a packet of information, attaches a heading to that packet, which, amongst other things, includes the address that that packet or chunk of information is to go to and sends that into a packet data network. The packet data network then routes that piece of information to the

appropriate destination. This type of service is particularly useful for terminal to computer communication where usually it is spent in silence, either reading the screen or deciding what to do next.

Packet transport allows the statistical sharing of the network amongst multiple users. This technology is being applied both in the business and residential environments. Many Bell operating companies are introducing packet services in the residential environment right now. Data is placed simultaneously with voice on the customer's existing local loop. This data may represent home information or home banking services.

The data in the form of packets is then routed to the appropriate home information or bank service. In the large business environment, digital capabilities are being introduced at an extremely rapid rate. Here digitized voice, data, and digitally coded video are multiplexed together; that is, combined together to make efficient use of telecommunications.

Exiting the customer's building typically is 1.5 million bits per second of information. The telephone network then fans out these bits to individual services desired by the customer. The result of all this is that the network becomes a huge, intelligent bit carrier. "A bit is a bit is a bit." These bits represent the mixture of voice, data, video, and image. This concept is called an Integrated Services Digital Network, and international groups are currently meeting to define the necessary network interface standards.

In summary, the telephone network is changing at a tremendous rate. Customers are becoming very sophisticated. What was once a network which carried only voice now routinely transports many different forms of information; that is, voice, data, video, and image.

And I thank you for your time.

Mr. CAMING. May I make one remark of a concluding character? As Dr. Weber has shown, and I might reiterate, both voice and computerized data or other nonvoice communications can be sent now in some cases alternately over the same telephone line or transmitted simultaneously, one under the other, as the customer may desire.

And it is sent in either analog or digital form. It seems that perhaps the critical question from a legislative standpoint would be whether it is a voice conversation; that is, you start out and you intend to speak to someone, what we call an aural acquisition under title III; or is it a data transmission or other nonvoice communication like facsimile—a nonaural acquisition; not whether it is analog or digitized, because when we place a call—and I think it bears reiteration—the call will generally be converted to a form that can be handled over the network, whether it is in analog or digitized format.

And then it goes out over the network in a series of links or circuits which join up. Now, these are almost always randomly selected, depending upon the particular routing of that call at that moment, the circuits that are then available and free to take the traffic, the volume of traffic at a particular time of day, and so forth.

And it can be and usually is a combination of analog or digitized circuits chosen at random and often without the telephone compa-

ny knowing it. So that the real focus should be on the nature of the conversation, rather than the means of transmission, which reflects the statement too that was stated by the Congress in the legislative history of the Foreign Intelligence Surveillance Act.

Senator LEAHY. Among the things that you have told me today, one of the things that pleases me is to hear your company's own concern about privacy. Do you have written policy guidelines that are given to, say, your operating personnel? Do you develop an ongoing privacy policy? I mean, technology changes all the time. Your company obviously is as aware as anybody in the world of how that is developing and also what would be the possible abuses there. Do you develop a policy as you go along?

Mr. CAMING. Yes; we have an extremely detailed type of orientation given to all employees on an ongoing and repetitive basis. For example, our Code of Conduct's first section is on privacy of communications.

And in recent years we recently amended it to make clear that protection of the communication and prohibition of any overhearing, except in the course of performance of duties, was to apply both to voice and data and other nonvoice communications. We stress that particularly in our recent revision. Now, our Code of Conduct is generally reviewed with the employee body as a whole, at least once a year, and a record very carefully made.

We also have—it has always been traditional to have—ongoing concerns for secrecy of communications, and any employee violation, for example, of privacy usually results in the most draconian penalties.

Senator LEAHY. Well, you still have times when the U.S. Government or, perhaps in some instances, the State government are going to request or require your cooperation, court orders, wiretaps, whatever. I was aware of some of that when I was a prosecutor. I am more aware of it now.

Has the U.S. Government's authority under our present law been clear enough as to what they can and cannot do when you have to determine to what extent you cooperate or you do not cooperate? Or do you find some difficulties in determining just how far you can or cannot go?

Mr. CAMING. I might say that in this area I have been the principal architect of policy, because I also have served as the chief company policymaker in this area for almost 20 years now. We have had no problems whatever, and I can explain why. We, first of all—and I have testified on that on a number of occasions before the Congress—provide very limited assistance to law enforcement. We act only when so directed by a specific court order, either in title III or FISA. And our assistance is limited to providing the cable and pair information that permits identification of the target's line, and a channel, usually between a terminal that would serve the listening post and a terminal that is in the same terminal that serves the target line. Then law enforcement has the responsibility of making the connection and also on the listening post side, placing whatever they wish.

When we battled in court, because there was a difference of interpretation of the law and it was very amicable but intense, as lawyers are, we went up to the Supreme Court of the United States

in the *New York Telephone Company* case before we would cooperate at all in a Pen Register situation without a title III order. We lost in a 5-to-4 decision.

All I can say is I like the dissenting viewpoints. But we then were required by that court decision to act in accordance with a court order that was issued usually in search warrant form. But it, too, had to contain a directive to us. After *Smith* v. *Maryland* was decided, the question was graciously raised by law enforcement, would we be interested in cooperating in Pen Register situations without a court order. And our answer was no. And we do request a court order for that, even though it may be legally permissible to voluntarily undertake rendering such assistance.

What we have adopted in order to maximize privacy of communications, since we are a common carrier and safeguarding communications is a very primary responsibility of ours, is to cooperate sufficiently to effectuate each wiretap, but only when a court so directs in precisely and in very limited fashion.

Now, I might say that the Department of Justice over the past 20 years or so has always been most sensitive to this viewpoint of ours and we have generally drafted and have in effect model orders which are presented to us, which very precisely limit our role in implementing either an order of a title III court or of foreign intelligence surveillance court.

Senator LEAHY. Do you see that type of sensitivity to privacy now with the breakup of AT&T with the individual companies, local, long distance, and so on? Is there an effort made to continue those policies?

Mr. CAMING. It is of course hard for me to definitively state what their existing intentions are, but to my knowledge——

Senator LEAHY. I understand that, but do you get the impression?

Mr. CAMING. To my knowledge—and I am very close to and I still hear from a number of them from time to time—they have generally maintained almost precisely the same policies. The dedication to privacy by the operating telephone companies of the Bell system was always most supportive and basic. And I think that in no significant respect will they deviate.

In fact, I know—we have written procedures, by the way, that are very detailed. Every "i" is dotted. Every "t" is crossed. And as far as I know—and I spoke last to them just before divestiture last fall—they continue to scrupulously adhere to the same policies they followed as Bell system operating companies.

Senator LEAHY. Would AT&T support protection for both voice and data if written into the law?

Mr. CAMING. We would strongly urge it. We urge that protection be afforded to all forms of communication where there is a reasonable expectation of privacy. It seems, particularly in this day and age, to make little sense to protect a voice conversation when my wife calls the grocer and orders a quart of milk, and yet when the Government may be dealing with a defense contractor or a company may be transmitting proprietary information or personally identifiable data there is not the necessary legal protection.

Senator LEAHY. I obviously agree with you on that. I probably will have as a result of this a couple more technical questions, and I would ask if I might be able to submit those to you.

Mr. CAMING. We would be very pleased to give you whatever help we can.

Senator. LEAHY. I appreciate your testimony here today and apologize for the Washington weather. Where is Basking Ridge?

Mr. CAMING. Basking Ridge is quite close to Morristown. It is 8 miles from Morristown and it is in a very pastoral setting and probably one of the most attractive Tibetan lamasaries east of Katmandu.

Senator LEAHY. OK. Well, thank you both very, very much.

Mr. CAMING. It is a pleasure, sir.

Senator LEAHY. We have Deputy Assistant Attorney General John Keeney from the Criminal Division of the Department of Justice. Could Mr. Keeney come forward, please.

Before we start I would note that we will insert in the record a letter from myself to Attorney General Smith of January 26, 1984, a response dated March 9, 1984, from Mr. Keeney, and another letter dated June 14, 1984.

[The letters referred to above follow:]

STROM THURMOND, S.C., CHAIRMAN
CHARLES McC. MATHIAS, Jr., MD
PAUL LAXALT, NEV.
ORRIN G. HATCH, UTAH
ROBERT DOLE, KANS.
ALAN K. SIMPSON, WYO.
JOHN P. EAST, N.C.
CHARLES E. GRASSLEY, IOWA
JEREMIAH DENTON, ALA.
ARLEN SPECTER, PA.
JOSEPH R. BIDEN, Jr., DEL.
EDWARD M. KENNEDY, MASS.
ROBERT C. BYRD, W. VA.
HOWARD M. METZENBAUM, OHIO
DENNIS DeCONCINI, ARIZ.
PATRICK J. LEAHY, VT.
MAX BAUCUS, MONT.
HOWELL HEFLIN, ALA.
VINTON DeVANE LIDE, CHIEF COUNSEL AND STAFF DIRECTOR
DEBORAH K. OWEN, GENERAL COUNSEL
SHIRLEY J. FANNING, CHIEF CLERK
MARK H. GITENSTEIN, MINORITY CHIEF COUNSEL

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, D.C. 20510

January 26, 1984

The Honorable William French Smith
Attorney General of the United States
Department of Justice
10th Street and Constitution Avenue, N.W.
Washington, D.C. 20530

Dear Attorney General Smith:

Recent newspaper and magazine articles have focused public debate on the question of whether federal government law enforcement agents may, as a matter of law, secretly and without a warrant or court order employ electronic surveillance of wire communication that does not involve the "aural acquisition" of information. (See, e.g., enclosed published materials.) Such communication would include, but would not be limited to, digital communication and any form of "pen register" or "touch tone decoder" device which is used to acquire from the contents of a wire communication the identities or locations of the parties to the communication, but which has been held to be outside the protections of the Fourth Amendment as well as the coverage of Chapter 119 of Title 18 of the United States Code (Chapter 119).

From published articles it would appear that the Deputy Assistant Attorney General for the Criminal Division has expressed some public views on this subject. According to reports he has indicated that as a matter of policy, in many cases the Department would advise seeking a warrant or court order. However, he did not appear to conclude that there was currently a statutory requirement for a warrant or court order to conduct electronic surveillance involving nonaural acquisitions.

On the other hand, there has been reported a contrary view of a Senate expert that the Foreign Intelligence Surveillance Act of 1979 (FISA) criminalizes the conduct of all such wiretaps -- whether for domestic law enforcement or foreign surveillance -- if conducted without warrant or court order. The argument is based on the provisions of section 109 of FISA, 50 U.S.C. 1809. That section makes it an offense to engage in electronic surveillance under color of law except as authorized by statute. The argument maintains that the nonaural electronic surveillance at issue falls within the definition of electronic surveillance in FISA and that Chapter 119 does not specifically provide a statutory exception for nonaural communication even though that section by its own terms does not make nonaural interception subject to that chapter's legal requirements.

In light of these inconsistent views of current statutory requirements, an attorney from my staff contacted the Department of Justice to ascertain whether the views of the Department were correctly reported and if not, what were those views. Apparently, the matter is currently under consideration, and the Department's answer is expected shortly. I currently am reviewing this question and would very much appreciate receiving the Department's written views on this question as expeditiously as possible.

Thank you for your attention to this matter.

Sincerely,

PATRICK LEAHY
United States Senator

U.S. Department of Justice

Criminal Division

Assistant Attorney General

Washington, D.C. 20530

MAR 9 1984

Honorable Patrick Leahy
United States Senate
Washington, DC 20510

Dear Senator Leahy:

The Attorney General has asked me to reply to your letter of January 26, 1984, concerning the Department of Justice's views on the question whether federal law enforcement officials may, as a matter of law, conduct warrantless electronic surveillance of wire communications when the surveillance does not involve the aural acquisition of the contents of such communications.

As you know, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. Sections 2510-2520 (Title III) does not govern the electronic and mechanical interception of wire and oral communications unless the interception accomplishes "the aural acquisition of the contents" of the communication. 18 U.S.C. Section 2510(4). As the legislative history of Title III makes clear, that statute "protect[s] the privacy of the communication itself and not the means of communication." S. Rep. No. 1097, 90th Cong., 2d Sess., 90 (1968), reprinted in [1968] U.S. Code Cong. & Admin. News, pp. 2112, 2178. The Supreme Court has recognized that interceptions that do not secure the "aural acquisition" of the contents of a communication, and thus do not "overhear" the substance of a conversation, are not within the scope of Title III. United States v. New York Telephone Co., 434 U.S. 159, 166-168 (1977).

Nonaural interceptions of wire communications, while not within the purview of Title III, may, in certain instances, be regulated by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. Sections 1801-1811 (FISA). Although the procedural provisions of FISA apply to electronic surveillance within the United States for foreign intelligence, and not for domestic law enforcement purposes, the definitional and criminal penalties provisions of the act appear to have a broader applicability. The procedural requirements of FISA specifically attach only to electronic surveillance, as defined in that act, when the surveillance is employed for the purpose of obtaining foreign intelligence information, but the criminal penalties section of FISA is nowhere limited to the intelligence gathering function. That section states that a person is guilty of an offense if he intentionally engages in "electronic surveillance" under color of law except as authorized by statute. 50 U.S.C. Section 1809(a)(1). An affirmative defense is provided for law enforcement officers who engage in electronic surveillance pursuant to a search warrant or court order. 50 U.S.C. Section 1809(b).

Since FISA requires a court order, but not a warrant, Congress presumably would not have made the defense applicable to law enforcement officers acting pursuant to both court orders and warrants had it not intended that

the criminal sanctions apply to electronic surveillance beyond the foreign intelligence gathering area. Support for this position is found in the House Conference Report on the bill that eventually became FISA wherein it was noted that House amendments to the bill "provide for separate criminal penalties in this act, rather than by conforming amendments to Title 18, for any person who intentionally engages in electronic surveillance under color of law except as authorized by statute. A defense was provided for a defendant who was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction." House Conf. Report No. 95-1720, 95th Cong., 2d Sess., 33 (1978), reprinted in U.S. Code Cong. & Admin. News p. 4062 (emphasis added). We would conclude, therefore, that a court order or warrant must be obtained whenever a surveillance technique employed in a domestic criminal investigation falls within FISA's definition of "electronic surveillance."

We do not believe, however, that 50 U.S.C. Section 1809 constitutes a statutory prohibition against all warrantless electronic surveillance involving nonaural acquisitions of communications because FISA's definition of "electronic surveillance" does not apply to all such communications. "Electronic surveillance," as defined in FISA, includes:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. Section 1801(f). All the definitions of "electronic surveillance" quoted above, except for subsection 1801(f)(2) limit the term by making it applicable when there exists "a reasonable expectation of privacy." Subsection 1801(f)(2) applies more broadly to a "wire communication," which is defined as "any communication while it is being carried by wire, cable, or other like connection." 50 U.S.C. Section 1801(l) (emphasis added).

As you probably know, however, many long distance calls today are transmitted partly by wire and partly by radio communications, and it appears that a warrant is not required for the nonaural interception of the radio or microwave portion of a combined wire-radio transmission. This is so because the radio or microwave portions of such communications are not governed by Section 1801(f)(2). They fall within either Section 1801(f)(1) or 1801(f)(3), both of which define "electronic surveillance" in terms of

an individual's expectation of privacy in the communication intercepted. As the Senate Report explains:

> Because most telephonic and telegraphic communications are transmitted at least in part by microwave transmissions, subdefinition [2] is meant to apply only to those surveillance practices which are effected by tapping into the wire over which the communication is being transmitted. The interception of the microwave radio transmission is meant to be covered by subdefiniton [3] . . . or by subdefinition [1] . . .

S. Rep. No. 604, 95th Cong., 2d Sess., 33 (1977), reprinted in [1978] U.S. Code Cong. & Admin. News, pp. 3904, 3934.

Thus, the question whether a warrant or court order is legally required to conduct a nonaural interception of the radio portion of a hybrid wire-radio communication is, in our view, dependent upon whether there exists a reasonable expectation of privacy on the part of the individual whose communications are to be intercepted. If there exists such an expectation, a search warrant or court order is clearly necessary. If however, the individual can claim no such justifiable privacy expectation in the communication, neither FISA nor the Fourth Amendment prohibits the warrantless interception of that communication. See Katz v. United States, 389 U.S. 347 (1967); Smith v. Maryland, 442 U.S. 735, 740-741 (1979).

In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as that set out above are not always clear or obvious. Consequently, while we do not believe that there is currently a statutory requirement that a court order or search warrant be obtained in all instances involving nonaural interception, it is the policy of the Department of Justice to obtain such an order or warrant when nonaural electronic surveillance techniques are employed and our analysis indicates there is a reasonable expectation of privacy.

We hope that this letter has clarified the Department's position with respect to the current legal requirements for nonaural interceptions. However, if we can be of any further assistance, please do not hesitate to contact me.

Sincerely,

Stephen S. Trott
Assistant Attorney General
Criminal Division

By: John C. Keeney
John C. Keeney
Deputy Assistant Attorney General
Criminal Division

U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General *Washington, D.C. 20530*

JUN 14 1984

Honorable Patrick Leahy
United States Senate
Washington, D.C. 20510

Dear Senator Leahy:

By letter dated March 9, 1984, the Department of Justice responded to your letter concerning warrantless electronic surveillance of wire communications when the surveillance does not involve the aural acquisition of the contents of such communications. On the third page of our response, we suggested that "many long distance calls today are transmitted partly by wire and partly by radio . . . and it appears that a warrant is not required for the nonaural interception of the radio or microwave portion of a combined wire-radio transmission."

We wish to make clear that we believe that the microwave radio portion of a telephone call is normally accompanied by a justifiable expectation of privacy. Consequently, a judicial warrant would be required for the nonconsensual interception of such calls.

We regret any confusion created by our former letter.

Sincerely,

STEPHEN S. TROTT
Assistant Attorney General
Criminal Division

By:

JOHN C. KEENEY
Deputy Assistant Attorney General
Criminal Division

Senator LEAHY. I would also ask Mr. Keeney, I do have a number of questions for you, a number of which were raised in the letter earlier, if you might summarize your statement, the whole statement will be made of course a part of the record. But if you might summarize it, then we could go into some questions.

STATEMENT OF JOHN C. KEENEY, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, ACCOMPANIED BY ALAN KORNBLUM, DEPUTY COUNSEL, OFFICE OF INTELLIGENCE POLICY, DEPARTMENT OF JUSTICE

Mr. KEENEY. Thank you, Mr. Chairman. Mr. Chairman, I have here with me Alan Kornblum, who is the deputy counsel for the Office of Intelligence Policy. He is here in the event that we might get into the sensitive intelligence area, but I accept as my responsibility for the Criminal Division to make the presentation and to respond to your questions insofar as they pertain to the criminal enforcement activities of the law enforcement community.

Mr. Chairman, I might say that I am particularly happy to be here today in view of the communications which we have had and to clarify what I think is a continuing question as to what we do in law enforcement in interceptions, in the communications area.

Now, on the subject of the interception of communications, Mr. Chairman, we have to consider the fourth amendment's provision with respect to unreasonable searches and seizures as well as the several statutory provisions relating to the interception of communications.

The primary statutory provision is title III of the Omnibus Crime Control and Safe Streets Act of 1968, which authorizes the interception of oral and wire communications where a warrant based on probable cause is obtained. Of some relevance is the provision in the Communications Act, 47 U.S.C. 605, primarily governing the interception of radio communications.

The statutory provision which this committee has expressed the most interest in is 50 U.S.C. 1801 et seq., the Foreign Intelligence Surveillance Act of 1978. The purpose of FISA is to regulate the use of electronic surveillance for foreign intelligence purposes. Despite the narrow purpose of FISA, Mr. Chairman, its definitional and criminal penalties provisions give the statute a broader applicability insofar as criminal enforcement authorities are concerned.

In some instances, FISA makes criminal the use of certain techniques by enforcement authorities without a warrant or court order that are not criminal if committed by persons not connected with law enforcement.

In my statement I discuss the applicability of FISA and title III to several investigative techniques used by law enforcement. These include use of Pen Registers, whose use without a court order, as Mr. Caming has pointed out, would violate FISA.

I also discuss the commonly used paging devices; recognizing that paging devices can take a variety of forms, my statement discusses three general categories. And I want to emphasize, Mr. Chairman, that I am not an expert on technology. I was a little bit overwhelmed by the presentation by AT&T and all I can talk about is

general principles in the situations that arise, and the technical context will just have to be molded to meet those principals.

Senator LEAHY. Do not feel bad. Everybody in my office is under strict orders, not from me but from more significant people in my office, not to let me near any of the computers, machines, even the data processors, because of the immediate damage that I might cause by trying to work them. When I really have something, even with our home equipment, that I cannot understand at all, I go to a higher authority, my 14-year-old son who patiently says, "Dad, now you have just got to pay attention this time."

"I am not always going to be around to help you, Dad. Pay attention when I am talking to you." [Laughter.] Go ahead.

Mr. KEENEY. Mr. Chairman, the first one I want to discuss is a tone only. That is a radio transmission which transmits a signal to a person who carries a beeper. The signal merely informs him that there is a message waiting for him and he has to call back to his answering service or to some other service that he has bought in order to find out what the message is. The message is usually a telephone number that he should call. Now, with respect to that, we conclude that no court order or warrant is required for us to intercept that tone.

With respect to a display pager, that is where a telephone is used to contact the paging company's computer, which then transmits the information by radio in digital form to the subscriber's pager which emits a beep which alerts the subscriber that he can display the message visually, the message frequently being the telephone number of the caller. Now, there we say that title III is not applicable, the reason being that there is no aural acquisition. With respect to FISA we find that it is applicable if there is a reasonable expectation of privacy and there frequently would be such an expectation in these situations. If there is an expectation of privacy, a rule 41, Federal Rules of Criminal Procedure search warrant based on probable cause would be sought if we wanted to obtain that information.

Another type is a tone and voice pager, Mr. Chairman. Here the caller attempting to reach the pager-subscriber is told to leave a spoken message. The message is held in the computer and beeped to the subscriber and then it repeats the spoken message. Here we conclude that title III is implicated because the message is acquired aurally and because it is transmitted in part by wire. And here, as I say, a title III application to a Federal court of competent jurisdiction and an appropriate order would be required.

I also discussed, Mr. Chairman, computer transmissions and their interceptions to some extent and apply the same—and explain that we in law enforcement apply the same principles with respect to computer transmission.

Mr. Chairman, my statement notes that in certain circumstances the acquisition of computer information without court process by a law enforcement officer acting "under cover of law" would be a crime, while the same conduct by a private citizen would not be.

I also note that this inequity could be partially remedied by the passage of S. 2940, the administration's computer crime bill insofar as accessing a Federal Government-related computer is concerned.

Mr. Chairman, I am acceding to your request and that completes my statement. I will try to answer your questions.

[The prepared statement of Mr. Keeney follows:]

PREPARED STATEMENT OF JOHN C. KEENEY

DEPUTY ASSISTANT ASSISTANT GENERAL
CRIMINAL DIVISION

Mr. Chairman and Members of the Subcommittee, I am pleased to be here today to present the views of the Department of Justice on the subject of interception of data communications. Since the Subcommittee is not considering any specific piece of legislation, I will attempt to describe briefly the existing laws and policies that we in the Department of Justice follow in this area. As you know, the laws governing interception of communications are complex and are of particular importance since they attempt to strike a balance between legitimate privacy concerns and the responsibility of federal officials to investigate and prosecute criminals. While we in the Department of Justice are ever mindful of the privacy rights of our citizens, we think it is equally important to recognize the importance of court-ordered interceptions of communications in investigating major crimes.

Any discussion of this area must logically start with Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. 2510 et. seq.). Title III regulates the "interception" of "wire communications" and of "oral communications." All three of these terms are defined in 18 U.S.C. 2510. The term "intercept" means "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." The Supreme Court has clearly held that activities, such as the installation and operation of a pen register to record the numbers dialed from a particular telephone, that do not involve the "aural acquisition," or overhearing, of the contents of a communication are not within the scope of Title

III, and hence Title III's requirements pertaining to the obtaining of a judicial warrant do not have to be followed.[1]

The term "wire communication" means "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception..." while the term "oral communication" means any spoken utterance "by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." These definitions of the types of communications covered by Title III should be kept firmly in mind because Title III actually applies only to certain categories of overhearings. Simply put, the requirements of Title III need only be followed when federal law enforcement officers seek to hear the contents of a communication made in whole or in part through a wire or similar transmission medium, or of any other oral communication -- such as in a private meeting between two persons -- in circumstances reasonably justifying an expectation of privacy.

There is another statute that applies and which operates to mandate that law enforcement officers obtain either a warrant or a court order before engaging in most activities involving the surreptitious obtaining of information. That statute is the Foreign Intelligence Surveillance Act of 1978, or FISA, 50 U.S.C. 1801-1811. The purpose of FISA was to regulate the use of electronic surveillance within the United States for foreign intelligence purposes, and the procedural provisions of FISA, which apply only to electronic surveillance employed for the purpose of obtaining foreign intelligence information, clearly reflect this goal. Nevertheless, the definitional and criminal penalties of the act have a broader applicability. For example,

---

1 See United States v. New York Telephone Co., 434 U.S. 159 (1977). In Smith v. Maryland, 442 U.S. 735 (1979), the Court held that the installation of a pen register also did not violate the Fourth Amendment.

50 U.S.C. 1809(a) provides that a person is guilty of an offense if he "engages in electronic surveillance under color of law except as authorized by statute."[2]. An affirmative defense is provided for law enforcement officers who engage in electronic surveillance pursuant to a search warrant or court order. Consequently, we have concluded that, unless otherwise authorized by statute, a court order or warrant must be obtained whenever a surveillance technique employed in a domestic investigation falls within FISA's definition of "electronic surveillance."

Permit me now, Mr. Chairman, to describe some of these surveillance techniques and state what we believe is required by way of a search warrant or a court order for their use.

Pen Registers

Although as I have indicated, the requirements of Title III have been held not to apply to the use of pen registers, and the Supreme Court has held that the Fourth Amendment does not require a warrant for their use, the FISA requires that law enforcement

---

2 The term "electronic surveillance" is defined in the FISA at 50 U.S.C. 1801(f). It means:

"(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

"(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;

"(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

"(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."

officers obtain a court order before using one of these devices. This results from the fact that the FISA definition of "electronic surveillance" does not contain any requirement for an "aural" acquisition of information. Rather, the second paragraph of the definition of electronic surveillance under FISA refers to the acquisition by electronic, mechanical, or other surveillance device of the contents of a wire communication. While a pen register would not appear to reveal the contents of a telephone communication since it records only the numbers dialed from a particular telephone, the term "contents" is defined in 50 U.S.C. 1801(n) to include the identity of the parties to the communication and the legislative history of FISA makes it clear that Congress intended law enforcement officers to obtain court orders before using a pen register.[3]

Pagers

Today many persons carry these devices so that they can be kept advised of attempts to reach them by telephone while they are away from their homes or offices. There are three common types.

First are "tone only" pagers. These devices emit a sound -- usually a "beep" -- caused by a radio transmission which serves to alert the user that he or she has a telephone call. The user of the "tone only" pager must then call his office or answering service to find out who called and what number he has been asked to call back. The overhearing of the "beep" by a law enforcement officer or the interception of the radio wave that causes the sound -- even if accomplished by means of special equipment to pick up the sound or radio wave at long range -- does not require either a warrant or court order. Title III does not apply since the contents of the communication are not overheard. FISA does not apply because it only applies to radio communications in

---

[3] This is true as well of a trap and trace device, which records the numbers of telephones from which calls to a particular telephone are dialed.

situations where there is a reasonable expectation of privacy. A person who uses a pager device which emits a "beep" can hardly be said to have such an expectation. Moreover the contents of the communication cannot be said to be overheard because the interception of the "beep" or of the radio wave that caused it would not tell law enforcement authorities either the number of the person who had called or the number that the person using the pager must call to obtain this information.

A more sophisticated type of pager is the "display pager." A caller attempting to reach the possessor of such a pager is instructed to touch tone his own telephone number or other message which is then received by the paging company's computer. The computer then transmits the information in digital form to the pager. Most commonly the pager will emit a "beep" which alerts the user that he can display the message, typically the telephone number of the person who called. Title III does not apply to the use of such pagers because the acquisition of the digital message is not an aural acquisition. Although the issue is not totally free of doubt, we think that persons using display pagers have a reasonable expectation of privacy. Thus, federal officers who intercept the transmission of the radio waves revealing the call back number should obtain a search warrant under the provisions of Rule 41 of the Federal Rules of Criminal Procedure. The provisions of the FISA would also appear to prohibit the interception of such a transmission without a warrant or court order.

Another type of even more sophisticated pager is the "tone and voice pager." A caller attempting to reach the possessor of such a device is told to leave a spoken message. The message is then held in the paging company's computer and, when the appropriate radio frequency is clear, it is transmitted to the pager. The pager then "beeps" to alert its user and then actually repeats the spoken message. In our view, the interception of such a message by law enforcement authorities would require a

Title III warrant because the repetition of the message by radio is simply a continuation of the original wire communication from the placer of the call to the user of the pager. Since the communication is in part aural and was sent in part by wire, it is a "wire communication" within the meaning of Title III and a Title III warrant should be obtained.

Mr. Chairman, that brings me to another area that I suspect is of concern to the Subcommittee in light of some of my statements at past hearings and as reported in the press. As a result of new technologies, many long distance telephone calls today are transmitted partly by wire and partly by radio. A Title III warrant is required for the aural acquisition of the contents of the call, whether the call was overheard by tapping into the wire portion of it or by intercepting the portion carried by radio waves, because the communication is, in part, a wire communication.

Some transmissions do not involve the human voice but consist of two or more computers transmitting information among themselves either through a wire or radio transmission. In theory, at least, federal law enforcement officers might have a need to obtain the information contained in a tiny fraction of these calls to aid in the investigation of certain types of crimes such as business frauds or money laundering. Getting this information would not involve an aural acquisition of the calls' contents so as to implicate the provisions of Title III. However, FISA would require that we obtain a court order or warrant before intercepting most of these communications. Section 1801(f)(2) of title 50, United States Code, defines "electronic surveillance" to include the acquisition -- including nonarual acquisition -- of the contents of any wire communication. Thus, this definition under FISA would require the obtaining of a warrant or a court order for the nonaural acquisition of information while it is being carried by wire.

Moreover, 50 U.S.C. 1801(f)(1) or (f)(3) would require a

warrant or court order for the acquisition of information while it is being sent by radio waves in all cases where there existed a reasonable expectation of privacy. We recognize that such an expectation often exists. Consequently, even before we in the Criminal Division became fully aware of the broad scope of FISA our position was, as a matter of policy, that if there was any question as to whether the parties had a reasonable expectation of privacy, a warrant should be obtained before intercepting a radio communication. This policy was, of course, dictated by the Fourth Amendment and the line of familiar Supreme Court cases making it clear that a warrant is required for searches in situations in which a person has a reasonable expectation of privacy against governmental intrusion.[4] Therefore, FISA merely stated as a matter of law our existing policy, and of course we will follow the law as well as our policy.

In conclusion, Mr. Chairman, I might note that the criminal provisions in FISA only apply to law enforcement officers inasmuch as they state that a person is guilty of an offense only if he engages in electronic surveillance "under color of law" except as authorized by statute. Thus, a private person who without authority makes a nonaural acquisition of information from a telephone line between two computers, or from a radio transmission between two computers for the purpose of personal financial gain does not violate either the criminal provisions in FISA or in Title III, while an FBI agent who does the same thing in the course of a complicated criminal investigation, is himself in violation of the law. We respectfully suggest that this inequity could be partially remedied by passage of S. 2940, the Administration's Computer Crime bill which would proscribe

---

[4] See, e.g. Katz v. United States, 389 U.S. 347 (1967). In its last term the Supreme Court held that the monitoring of an electronic tracking device or transponder, which enabled law enforcement officers to track the location of an object inside a private residence required a warrant. United States v. Karo, _____ U.S. _____ No. 83-850 (July 3, 1984).

accessing computers operating in interstate commerce as part of a scheme to defraud. As for any additions to our laws regulating the authority of law enforcement officers to make nonaural acquisitions of information we would submit that this is a very complex area of the law already and that any changes deserve extraordinary review and discussion.

Mr. Chairman, that concludes my prepared remarks and I would be happy to answer any questions at this time.

Senator LEAHY. Thank you. If I can just kind of walk you down through some examples just to make sure I understand, so as to make the hearing record more understandable to a lot of us. You said in your letters to me and your statement that the requirements of title III only need be followed when a law enforcement officer seeks to overhear the contents of an aural or wire communication, which is, basically, as I understand it, we have the example of two people having a conversation. Let me give you some more examples and tell me whether title III would be applicable.

Suppose you have two people and they are talking via long distance telephone. Their voices are being converted into a digital form for transmission, what we were discussing earlier this morning. Would title III cover the acquisition of communication in digital form?

Mr. KEENEY. I think it is a unitary transmission. We would seek a court order, a title III court order in that situation, and if a private individual intercepted the digital we would seek to proceed criminally against the individual and at least get a court test on the issue.

Senator LEAHY. Now, of course, title III would apply to a private individual. It would not apply to a FISA situation.

Mr. KEENEY. I do not understand the question. FISA, in our view, is an entirely separate situation, in many respects much broader than title III insofar as the restrictions on law enforcement authority are concerned. FISA, on the other hand, has little applicability to nongovernmental authorities.

Senator LEAHY. That is what I mean. Now, what if you had two people communicating via the same telephone circuitry but they were using keyboards and video display terminals? Would the interception of that material be covered by title III?

Mr. KEENEY. Telephone usage in video display.

Senator LEAHY. But they are not talking at all. They are just using keyboards, video display terminals. In other words, suppose I want to send a memo to one of my offices in Vermont. We type up the memo and use the telephone circuitry, press a button and the memo shoots out up there. Somebody up there looks at the memo and makes a response. It again comes back to my video display terminal. We have not talked at all, but we have obviously communi-

cated back and forth, but we are doing it by keyboards and video display terminals. Would the interception of that be covered by title III?

Mr. KEENEY. No, sir, but it would be covered by FISA.

Senator LEAHY. It would be covered by FISA but not by title III.

Mr. KEENEY. Right.

Senator LEAHY. OK. Now let us go to another situation. There are no people at all at the keyboard.

Mr. KEENEY. I am talking now, if the interception were made by law enforcement under the color of law, it would be covered by FISA, yes. I just wanted to clarify that answer.

Senator LEAHY. Then again, in asking these questions I realize it calls for some quick, off the cuff legal decisions; and, naturally, you are going to get a copy of this transcript, and, when you look at it, if the question is not clear enough or you want a clarification, just let me know and we will——

Mr. KEENEY. Yes, sir. I might just say generally that most of the things that were being discussed by the AT&T representatives today insofar as data transmission is concerned would involve an expectation of privacy and I would believe that FISA is implicated and would be available again to Federal law enforcement. Again, its applicability is limited.

Senator LEAHY. What about if people hooked into a video teleconference that we saw pictures of today? What about the interception of the images being transmitted by a telephone network? Is that covered by title III, just their images.

Mr. KEENEY. Images without the voice, my view would be no.

Senator LEAHY. Now, what about the interception of electronic mail messages? That is something we are now getting into, ZAP mail or whatever they call it?

Mr. KEENEY. Electronic mail messages that are sent out by wire?

Senator LEAHY. Yes.

Mr. KEENEY. No title III, but FISA would be implicated.

Senator LEAHY. What did you say about FISA?

Mr. KEENEY. FISA would be implicated. We would be precluded from intercepting that without getting a court order or a warrant.

Senator LEAHY. OK. Now I am seeing more and more private telephone networks; a company with branch offices now sets up their own private telephone line, microwave or whatever, back and forth. Now, suppose you have two people—that first example I gave you—two people talking and they are talking on a private network. It is not regulated as a common carrier by the FCC.

Would the interception of even an analog communication in that form be covered by title III.

Mr. KEENEY. By analog you mean an aural conversation?

Senator LEAHY. Yes.

Mr. KEENEY. If there is a wire implicated and if it goes in interstate commerce, I think it would be covered, Senator. There may be ramifications or variations of that questions where——

Senator LEAHY. This is not a common carrier. This is totally a private situation.

Mr. KEENEY. I would have to check it, but I do not think that the fact that it is not a common carrier has any effect as far as the

applicability of title III is concerned, as long as it is in Interstate Commerce.

Senator LEAHY. What are the sanctions for a private party who intercepts a communication in violation of title III?

Mr. KEENEY. I think it is 5 years.

Senator LEAHY. Is that a misdemeanor?

Mr. KEENEY. No; that would be a felony.

Senator LEAHY. What is the difference between the definition of wire communication in FISA from that of title III?

Mr. KEENEY. FISA is much broader. It includes the data transmission that we have been talking about here as well as verbal communications that go out over a wire and verbal communications that do not go over a wire, but where there is an expectation of privacy.

Senator LEAHY. But FISA is not applicable to interceptions by private parties.

Mr. KEENEY. It is not. There is no Federal sanction that I am aware of for interception of data transmission that would violate FISA. But there is, as I keep emphasizing, there is a proscription and a penalty for that being done by law enforcement people.

Senator LEAHY. So FISA really goes into a lot more of the technology, but it is Government directed.

Mr. KEENEY. Yes, sir.

Senator LEAHY. Would it create a problem for law enforcement if we amended the definition of wire communication to include all common carrier communications which are transmitted at least in part by wire?

Would that be a problem if we put that in?

Mr. KEENEY. Can I have that again, Senator?

Senator LEAHY. In title III we have wire communications, as I understand it—and correct me if I am wrong—and this includes all common carrier communications which are transmitted at least in part by wire.

If we put that definition into FISA, does that create a problem for law enforcement? Or is that the definition in FISA?

Mr. KEENEY. I think the reverse would be creating a greater law enforcement burden. I guess I still do not fully understand the question. I am sorry, Senator.

Senator LEAHY. I am having a wee bit of a problem with it myself.

Mr. KEENEY. Do you have the thought of amending FISA so as to make it applicable to everybody or do you—are you just talking about amending title III? If you are amending title III, the only thing you achieve is you change the type of warrant or order that the Federal Government has to get for law enforcement purposes. If you change, broaden the applicability of FISA, you are bringing in under the sanctions private individuals as well as people acting under the color of law.

Senator LEAHY. Why do I not yield to my chief counsel, John Podesta, here.

Mr. PODESTA. The definition of wire communication in FISA includes only the communication while it is carried on the wire. There is no requirement that a reasonable expectation of privacy be found in that circumstance. I think there is an assumption that

there is a reasonable expectation of privacy when there is a communication by wire and law enforcement must get a court order.

On the other hand, in a common carrier situation when communication is carried partly by wire and partly by radio-microwave, if you intercept the communication during the radio-microwave portion you must find a reasonable expectation of privacy.

Would it be a problem for law enforcement to cover at least all common carrier communication situations in FISA that are carried at least in part by wire and in part by radio-microwave?

Mr. KEENEY. Well, if there is a reasonable expectation of privacy, you bring the court in. If there is a reasonable expectation of privacy in any part of the communication, we have got to get a search warrant with all the requirements, the specificity, and so forth, in that.

If the transmission is partly by wire and partly by microwave, that would implicate title III because of the fact that if there is—I am assuming now we are talking about an aural conversation.

Mr. PODESTA. Unless it is a data transmission.

Mr. KEENEY. Oh, you are talking about data transmission. Data transmission, I would say, there is a reasonable expectation of privacy normally in those situations, and if there is, then we would have to get a rule 41 search warrant.

Mr. PODESTA. I think what the question is ultimately asking is, Are there circumstances where there is no reasonable expectation of privacy?

Mr. KEENEY. I think there are.

Mr. PODESTA. Could you define what those are in a common carrier situation.

Mr. KEENEY. In the common carrier situation I just do not know. I just do not have the technical expertise. It seems to me conceivable that you could be broadcasting even in a common carrier situation where the ability to intercept is widely known and is widely practiced and therefore the expectation of privacy would not be reasonable.

Senator LEAHY. Like the Kansas Supreme Court's ruling on the portable telephones, that there is no reasonable expectation of privacy. Somebody overheard a conversation on one of these portable phones you walk around with.

Mr. KEENEY. Portable phones, I understand, Senator, your neighbors can pick up the conversations. You walk out into your yard and take a phone call and everybody in the neighborhood can hear the conversation. I am told that is true.

If it is true, I do not see how you can have a reasonable expectation of privacy.

Senator LEAHY. What about the person on the other end of the line, though, that does not know you are walking around with a portable phone? Do they not have a reasonable expectation of privacy?

Mr. KEENEY. I suppose they do. I suppose they do.

Senator LEAHY. I do not know the answer to that.

Mr. KEENEY. All I am trying to suggest here with respect to reasonable expectation of privacy and the concomitant need to get a rule 41 search warrant is that you have to decide them on a case-by-case basis, and with the expansion of technology, it is hard to

cover particular situations. You just have to isolate the facts of a particular transaction.

Senator LEAHY. I am going to submit for the record some questions on computer software that now can be transmitted via telephone. It is becoming a commercial question because of private sector interceptions of computer software being transmitted and what are some of the problems there.

Mr. KEENEY. Well, it is being transmitted by wire, the computer software information is being transmitted by wire.

Senator LEAHY. Yes. And what would be the law governing the interception of these transmission either by Government or an industrial interception, an industrial pirate.

Mr. KEENEY. Well, the industrial pirate would possibly come within the wire fraud statute if in fact it was going interstate. And the actual—if some of the computer crime legislation that is up here on the Hill now, particularly the administration's bill, the accessing of the computer by someone not authorized to access would be at least a misdemeanor.

Senator LEAHY. In fact, I will pass on after this based on the hearing today some more questions for the record. I might say in that regard, incidentally, I appreciate very, very much the response that you have given to my previous letters. It was very thorough, extremely helpful to me and I believe extremely helpful to the Members on both sides of the aisle here. The answers are very professional and very thorough and I appreciate it very much.

Mr. KEENEY. Thank you, Senator.

Senator LEAHY. Irrespective of the state of the law today, are you aware of a department policy that would encourage the maintenance of a distinction between aural and nonaural transmissions in title III?

Mr. KEENEY. The distinction between aural and nonaural transmissions? Nonaural are normally not covered by title III.

Senator LEAHY. No. But are you aware of a policy decision in the department that would encourage the maintenance of a distinction? There is a distinction today, but would encourage the maintenance of a distinction between them as opposed to some here on the Hill who would like to do away with the distinction.

Mr. KEENEY. Well, let me just say in that regard, Senator, I am not aware of any distinction. What I am aware of, though, is a reluctance to tinker with title III. It is a very effective law enforcement tool and we have made great inroads with it in organized crime and particularly in the narcotics traffickers. And we would be very sensitive to any amendments that would lessen our ability to use what we consider to be a very effective tool.

Getting back to your basic question, I do not know of any firm, set policy that would automatically put us in opposition to an expansion of title III to cover nonaural, data transmission materials.

Senator LEAHY. I may possibly have some other questions on FISA. Some of the questions that I have asked and would be interested in I already asked them wearing another hat over in the Intelligence Committee. And they would be of the nature that I would not ask in an open hearing.

In any event, I think that pretty well covers the questions I have. I find the area is somewhat more complicated than I thought when

I first started out. But I also am concerned that we not get, we, those of us who have to write or propose these laws, not get so concerned about a technology that is expanding and changing so rapidly that we do nothing. I think the basic principles that you have referred to and others have referred to, the expectation of privacy, give us a good place to start and determine how to do that to maintain the average person's expectation of privacy without creating undue hinderances whether to law enforcement, intelligent services, or anything else. I think we have worked very hard to get a balance today. I think we can maintain a balance, but I also think that the current law is behind the times in some regard.

Mr. KEENEY. Senator, I agree with you with respect to the current law being behind the times insofar as the scope of its coverage. I think insofar as you and other Members of the Congress are sensitive about law enforcement's possible misuse of these sensitive techniques, I hope I have demonstrated today that the laws as they exist have us pretty well under control.

Senator LEAHY. I do not have problems with that. I spent 8½ years in law enforcement and I have—I am well aware there are problems that law enforcement operate under. I am also well aware that most law enforcement agencies like clear-cut lines of what they can and cannot do and will operate within that. I see a lot of other areas coming up here including, quite frankly, areas outside law enforcement, the private areas, the areas of commercial theft, and so forth, and want to make sure that we are not leaving loopholes available there.

But I will submit further questions. I do appreciate your testimony today and I do appreciate very, very much the cooperation I have received so far.

Mr. KEENEY. Thank you, Senator.

Senator LEAHY. I am going to recess for about 3 minutes to return one phone call and then I will be right back in.

[Brief recess.]

Senator LEAHY. Next we have a panel with Ronald Plesser, attorney with Blum, Nash & Railsback, here in town. Mr. Plesser was general counsel to the U.S. Privacy Protection Study Commission. Presently, he is the chair of the Privacy Committee of the Individual Rights and Responsibilities section of the American Bar Association. We also have with us Mr. Steven Schachman of Bell Atlantic Mobile Systems, also of Basking Ridge, that idyllic area of what we refer to in Vermont as one of our nicer Southern States; Mr. Plesser, if you could start and then we will go to Mr. Schachman. One of the things, I told Mr. Plesser, one of the questions that I am going to be going into and the nature of the questions is that there are so many pessimists in the privacy field who worry that technology is going forward so rapidly that neither Congress nor the American people are ever going to bring our laws and social norms in line with the problems, the delay or time lag in adopting legislation. I just want to know if you think the pessimists are right.

Go ahead and begin any way you would like, and then we will go to Mr. Schachman, and then I will go to questions.

STATEMENTS OF RONALD L. PLESSER, PARTNER, LAW FIRM OF BLUM, NASH & RAILSBACK, WASHINGTON, DC; STEPHEN SCHACHMAN, BELL ATLANTIC MOBILE SYSTEMS, BASKING RIDGE, NJ; AND MARVIN S. COHEN, ON BEHALF OF THE CELLULAR COMMUNICATIONS INDUSTRY

Mr. PLESSER. We will handle that tough question a little later, Senator. It is a pleasure to be here. I submit my statement for the record and I will be relatively brief in my comments because I think that the witnesses before me have essentially made the case, which is AT&T, I think, which is the people who are really primarily responsible for handling the system say that there is confusion. They do not understand it and they think there should be some clarification in the law.

I think that is a pretty strong statement, not only that they agree with it but the statement was that they urged it. I think there is no question that the word aural in title III is very limited in light of where the technology has taken us and it is clear that digital communications are not covered technically under title III.

And the assistant attorney general, the deputy assistant attorney general also made the case because, first of all, he said one thing that I do not know so much that I disagree with him, but I think that he was not being totally forthright. He said that if a private person would intercept digital communications that the U.S. attorney would prosecute that case. That may or may not be their intent. They tried it in 1978 in the *Seidlitz* case, which is cited in my materials. The Fourth Circuit Court of Appeals said that title III could not apply under—that digital communications could not be prosecuted under title III and threw the case out.

I have no idea what has happened since 1978 and now to change the opinion of the Department of Justice, but cert was denied on that case and I would suggest that the same result would happen now.

My approach to this this morning is not that the criminal division is good or bad. I think there is a little sense of being oversight. The real question is the holes in the statute. It may be—and we can argue for the second that FISA has a certain amount of control over the Federal establishment. But there is no question from listening to the testimony this morning that there is absolutely no control on State officials who have a great deal of responsibility prosecuting laws; most of the State statutes are identical to title III, which also have aural communications, so that the intercept of digital communications by State officials is essentially a State law enforcement on police, which is the bulk of law enforcement in this country, is not protected by any statute.

And, second of all, the point, Senator, that you made in terms of private individuals, that their interception of other activity is not protected. I am not an expert, but I think if you go back to 1968 when the Safe Streets Act was passed, one of the concerns was not just the police activity, but at that time I think it was the concern that there were these spy shops on every corner where people could buy this very sophisticated intercept technology themselves, that private individuals could do it, and I think that statute very strongly was aimed at curbing the activities of private individuals,

and I think the advent of the technology at this point has essentially made that impotent. There is no activity.

I think in simple summary there are tremendous holes in communications privacy today, not only the aural problems, but also the question of common carrier. Traditionally all communications were carried by common carrier. Today as we get into sophisticated electronic mail systems and other types of activities, which are not common carrier activities, a lot of those protections are gone.

If I send a letter to a friend in California through the U.S. Postal Service—that letter, by statute and even by some constitutional concepts—I have an expectation of privacy. A warrant is needed if that letter is to be intercepted, even if there is a mail cover to see who I am sending to. There has to be some kind of warrant.

If I send it on electronic mail, not only is there not any intercept problem, but the electronic mail company simply is under no restriction whatsoever in turning the information over to the Government. And the U.S. Government has on occasion, recently within the last year, used subpoenas to attempt to get an electronic mail product from electronic mail companies.

Those companies have resisted in every case and forced them to go to subpoenas and have litigated the cases and have won the cases so far only through attrition, not through court order. So I think there is really a second issue that is almost equally important as the intercept in terms of what are the responsibilities of these new people who handle information who are not common carriers, and electronic mail, I think, is one of them.

Listening to the conversation this morning, too, I think focuses on a problem. I think expectation of privacy is very much like beauty. I think it all depends on who is beholding it in terms of how it is defined. And I think the *Kansas* case that you referred to, and I think my colleagues on the panel will talk about a little bit more in the *Executaphone* case, in the cordless telephone case. This indicates how courts vary in their view of it.

The Supreme Court of Kansas felt that there was no expectation of privacy and said, but we are not handling the situation. We are not dealing with the other end of the telephone; you know, the fellow who has made it on a land phone. How do you handle that?

Senator LEAHY. Who normally would be expected to have an expectation of privacy.

Mr. PLESSER. Absolutely. And also does that mean that your expectation of confidentiality is dependent upon reading the eight-point-type notice in the box that it can be picked up by a regular FM carrier. I think to require the expectation of privacy to be dependent on that kind of technical—did they read the notice or did they not—does it make a difference that a notice was in the cardboard box or not?

What if you got it as a Christmas present and it was just in a stocking and somebody took it out of the box? Does that then change the constitutional protections that are available to you? I think maybe if I can now slide into your question in terms of the pessimism that we in the privacy community—I was general counsel of the Privacy Commission and I think in terms of looking at those recommendations, I think I feel that we did a pretty good job,

that I think that a lot of it has not been thrown away by technology.

Senator LEAHY. I think the issue is pretty much the same.

Mr. PLESSER. I think the problems are pretty much the same. I think that what happens is that there are new players and new institutions, and I think the electronic mail example is one. I do not think 5 years ago or now 7 or 8 years ago, when we wrote the report, we really conceived of somebody like an electronic mail carrier who was taking information, relaying it, looking like a common carrier, acting like a common carrier, but not a common carrier.

I do not think we really focused on those kinds of problems, and I think Congress has a continuing responsibility to look at those issues. I am really not pessimistic about it; I just think there is going to be more work for all of us in terms of the technology. It is going to be constant. We are never going to be able to write a law that is going to forever match technology. It is going to be a constant process of growth and development.

Senator LEAHY. You do not see that as a reason to throw up your hands and not do anything?

Mr. PLESSER. Absolutely not. I mean, I think it is part of the growth curve and sometimes maybe the law could even get a little ahead of technology. Sometimes technology gets ahead of the law. The very narrow problem that we are talking about today, this question of aural communication and essentially expanding it to cover digital, just seems to me almost noncontroversial, and for the Justice Department to say there is no issue, when AT&T comes up here and says, yes, there is an issue and it is confusing and we need clarification, I think is a very important point.

Senator LEAHY. Well, you saw the March 9 response they made to me regarding DOJ's legal requirements for nonaural interception. I take it you do not agree with that?

Mr. PLESSER. Well, I mean, you can agree with it or you can not agree with it. I mean, essentially they are saying they are covered by FISA. My reaction to that is, one, great. How about all the State officials? How about all the private parties? There is a vast number of people out there about whom there should be concern who are not even approached. And of course the Department of Justice does not contend that.

Second, FISA grew out of a particular environment, and I think it is not for me, or certainly the time, to evaluate FISA, but the process in FISA is simply an ex parte procedure where officials have to go to a court that is essentially a secret court. I am not arguing about the veracity of that or the need for that or the validity of that for foreign intelligence activity, but when you start talking about agencies doing domestic activity, essentially domestic activity, and then to rely on the privacy being totally protected because of FISA, I think you miss the point.

There are no standards. Those warrants are essentially automatic, which may be fine in foreign intelligence but I do not think should apply in the kinds of areas primarily that we are talking about, which are different types of intercepts.

And so I think simply to rely on FISA may be—I mean, assuming that they are right, it is OK as far as it goes. I do not think it

takes it very far. There are no standards, and the real problem—and maybe this is not directly on the testimony this morning, but again it is a problem of not even the intercept problem.

The Department of the Treasury has issued some regulations recently that I have not checked on in the last couple of weeks. I assume they are not yet in final, but they have been in proposed form where every bank has to transmit to the Treasury Department data tapes of every foreign transaction handled by that bank. That is it, every foreign transaction. So if you send a money order to somebody in Ireland or Italy or wherever—not a money order, but a check, that is going to be recorded and sent to the Federal Government.

I do not think that anybody had—this is—and if you use wire communications for the transfer of those financial transactions, the Treasury Department is proposing that that all automatically be transferred. They are not intercepting. They are just taking.

And I think there are some broader issues of what right they have to the records in addition to the technical intercept that really need to be looked at.

I will continue answering questions.

[The prepared statement of Mr. Plesser follows:]

Prepared Statement of Ronald L. Plesser

Mr. Chairman, members of the Subcommittee, my name is Ronald L. Plesser and I am a partner with the law firm of Blum, Nash & Railsback, Washington, D.C. and I am here on my own behalf. I first became associated with information policy issues in 1972 when I became Director of the Freedom of Information Clearinghouse, a project of the Center for Study of Responsive Law. During that period of time, I litigated many cases under the Freedom of Information Act, several of which involved issues of access to records where personal privacy was a significant issue. I was General Counsel to the United States Privacy Protection Study Commission ("Privacy Commission") from 1975 through 1977. Since that time I have been in the private practice of law in Washington, D.C. representing a broad range of clients in the freedom of information, privacy and information technology areas. I have served as Co-Reporter to the Drafting Committee of the National Conference of Commissioners on Uniform State Laws in connection with the preparation of a State Model Information Practices Code. In addition, I was a Consultant to the National Telecommunications and Information Administration in conjunction with their consideration of the Privacy Commission's recommendations during the Carter Administration. I have written and spoken frequently on privacy and am currently an adjunct professor at the George Washington University School of Law.

My testimony today will be concerned with in view of rapid technological advances in telecommunications and computer science whether existing law on interception of wire and radio communications adequately protects the rights of privacy. This issue raises the larger question of whether our laws have kept pace with technology. I believe that in the area of communications privacy they have not. First, is the area of unauthorized interception where digital data transmissions by and

large are not protected by current wire tap statutes. Secondly, and of equal importance is the question of what are the rights of users in connection with these new technologies. Technology has outstripped our laws on interception, but it has also rendered impotent the expectation of privacy a person may have concerning government access to communication with the permission of the recordkeeper.

A. Communications Privacy

Government agencies cannot outside of Fourth Amendment protection intercept personal communications such as mail or telephone communications. In Berger v. New York, 388 U.S. 41 (1967), the Supreme Court struck down state statutes allowing eavesdropping based on ex parte orders of a court.

The Supreme Court then in an historic decision held that the Fourth Amendment to the U.S. Constitution required judicial authorization prior to electronic surveillance of public telephone booths. Katz v. U.S., 389 U.S. 347 (1967).

Following those decisions, the Congress has enacted two Federal statutes which directly affect electronic two-way communications. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (1968) imposes criminal sanctions against the interception of wire communications and regulates wiretapping by law enforcement authorities. Title III may be severely limited in the context of data transmission since it defines "intercept" as the "aural acquisition of the contents of any wire or oral communications" and the word "aural" probably does not cover textual or digital messages. One court has held that Title III does not apply to interception of computer transmissions because no "sounds" are involved. U.S. v. Seidlitz, 589 F.2d 152, 157 (4th Cir. 1978), cert. denied, 441 U.S. 922 (1978). From a technological perspective this is not a real distinction, since many telephone conversations may be digitized during at least some part of their transmission.

Moreover, where the electronic pulse is sent over a non-common carrier like cable television, the transmission may not be covered by Title III since Title III has been extended only to common carriers. 18 U.S.C. § 2510(1) (1968). See also United States v. Christman, 375 F. Supp. 1354 (N.D. Cal. 1974).

Section 605 of the Communications Act prohibits unauthorization interception of some signals. 47 U.S.C. § 605 (1976). This section is of limited effect since most of its provisions relate to over-the-air services. This section only prohibits an operator from intercepting and divulging messages to unauthorized third parties. Bubic v. United States, 384 F.2d 643 (9th Cir. 1967); United States v. Russo, 350 F. Supp. 55 (E.D. Pa. 1966).

While not covered by Title III, nonaural interceptions by law enforcement personnel are generally subject to the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801-1811 (FISA).

The Department of Justice views FISA as requiring a court order or warrant requirement on law enforcement personnel who are intercepting a "wire communication" "while it is being carried by wire cable, or like communication." The requirement of a court order or warrant for the nonaural interception of a radio or microwave transmission only exists where "a person has a reasonable expectation of privacy and a warrant would be required for the law enforcement purposes." Therefore, the protection provided by FISA for the radio or microwave portion of a combined wire-radio transmission, is coextensive with the protection provided by the Fourth Amendment.

The legal protections against unauthorized acquisition of digital communications are left largely to case-by-case determinations by the federal courts of whether there exists a reasonable expectation of privcy. The Court of Appeals decision in Jabara v. Webster, 691 F.2d 272 (6th Cir. 1982), cert. denied, _____ U.S. _____ (1983) demonstrates that the government's technical ability to intercept and interpret electronic

communications may be enough to defeat a person's reasonable expectation of privacy.

What this means is that the law may allow a vast amount of information transmitted partly by wire and partly by microwave to be acquired by goverment agents without a warrant or court order.

In addition to the gap in the law for digital transmission there is a gap for broadcast or oral as against wire transmission. This gap has been brought into focus by the use of cordless telephone. A cordless telephone is a device which permits you through a walkie-talkie type device to make and receive telephone calls up to a radius of approximately 700 feet from the base unit. The Supreme Court of Kansas has held that a user of a cordless telephone has no expectation of privacy when using the cordless phone and that private or police interception of such transmission does not violate Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. § 2510. Left unresolved is the expectation of confidentiality of persons on the other end of the line who believe that they are simply talking on a telephone. Kansas v. Howard, 679 P.2d 197 (Kan. 1984).

Therefore, the telephone conversations of users of cordless phones may be intercepted by police or others with no legal impediment. This I believe is a technological development not envisioned by the framers of the Constitution or Title III.

B. Privacy in General

In examining privacy in light of new technology, a review of the state of Fourth Amendment rights will help view the principles of privacy. This examination inevitably leads to the conclusion that the Constitution gives little, if any, protection to an individual and that we must look to legislative solutions, government mechanisms and Congressional oversight to protect the interests of privacy in our society.

The Privacy Commission's ability to conceptualize the problem it was trying to face in looking at an individual's right

to control information maintained about individual's right to control information maintained about individuals was facilitated by a case entitled Miller v. U.S., 425 U.S. 435 (1976) issued by the Supreme Court in the midst of the Privacy Commission's deliberations. The Miller story still had two lessons which are still of importance. First, the Fourth Amendment probably cannot survive the technological age and, second, that only by the protection of the rights of those in contact with the law can we protect the rights of all. Mitchell Miller's story bears repeating. An agent from the U.S. Treasury Department's Bureau of Alcohol, Tobacco and Firearms suspected Miller of direct involvement in two events, a seized truck and a warehouse fire which indicated illegal manufacture of alcholic products. Two weeks later, the agent presented grand jury subpoenas to the two banks where Miller maintained accounts. Without notifying Miller, copies of his checks and bank statemnets were either shown or given to the Treasury agents as soon as they presented the subpoenas. The subpoenas did not require immediate disclosure, but the bank officers nonetheless responded at once.

After he had been indicted, Miller attempted to persuade the court that the grand jury subpoenas used by the Treasury Department were invalid and, thus, the evidence obtained with them could not be used against him. He pointed out that the subpoenas had not been issued by the grand jury itself, and further, that they were returnable on a day when the grand jury was not in session. Finally, Miller argued that the Bank Secrecy Act's requirement that banks maintain microfilm copies of checks for two years was an unconstitutional invasion of his Fourth Amendment rights. The trial court rejected Miller's arguments and he appealed.

The Fifth Circuit Court of Appeals also rejected Miller's claim that the Bank Secrecy Act was unconstitutional, an issue that had already been resolved by the U.S. Supreme Court in 1974. The Court of Appeals agreed, however, that Miller's

rights, as well as the bank's, were threatened and that he should be afforded the right to legal process to challenge the validity of the grand jury subpoenas. The Court of Appeals saw Miller's interest in the bank's records as deriving from the Fourth Amendment protection against unreasonable searches and seizures which protected him against "compulsion production of a man's private papers to establish a criminal charge against him."

On April 21, 1976, a fateful day for personal privacy, the U.S. Supreme Court decided that Mitchell Miller had no legitimate "expectation of privacy" in his bank records and thus no protectible interest for the Court to consider. The Court reasoned that because checks are an independent record of an individual's participation in the flow of commerce, they cannot be considered confidential communications. The account record, moreover, is the property of the bank, not of the individual account holder. Thus, according to the Court, Miller's expectation of privacy was neither legitimate, warranted, nor enforceable.

Since the Privacy Commission's report, the Congress enacted the Right to Financial Privacy Act, which to a limited extent, gives depositors some standing to challenge Federally-issued subpoenas. The Supreme Court's conclusion that Miller could do nothing to protect records about him, however, has not changed. But for the promise of legislative solutions individuals have less and less control over information maintained about them. The Constitutional protections of the Fourth amendment continue to be eroded and soon little will be left. This is now demonstrated by the activities of the Treasury Department in seeking the disclosure of all foreign bank transactions undertaken by U.S. banks.

In computer activities there are no Fourth Amendment protections. Searches of the records of individuals are no longer limited by the word resonable as envisioned by the framers of the Constitution. The technology of computers have sanitized

search and seizures. Goverment-wide match programs for example, search information about individuals to the same end as if a government agent broke into your house and rifled your papers. But because you can't see it and because the ends are justifiable, the Fourth Amendment is deemed irrelevant. The Fourth Amendment is fast becoming a dead principle in light of electronic data transmission and other potential areas of access to private information.

Senator LEAHY. Thank you, Mr. Plesser.
Mr. Schachman.

STATEMENT OF STEPHEN SCHACHMAN

Mr. SCHACHMAN. Thank you, Senator. I am here today on behalf of the Cellular Communications Industry Association, which is our national cellular telephone trade association. I have submitted my testimony and I also will try to briefly summarize that testimony.

With me today is Marvin Cohen who is counsel to our association. Cellular is a new service that uses state-of-the-art technology to provide mobile telephone service on a greatly expanded basis over prior technologies.

Makers or recipients of cellular telephone calls have the same expectation of protection from unlawful interception as do makers or recipients of conventional land-line telephone calls. Indeed, one party to a telephone call may not even know that the other party is using a cellular telephone. Therefore, cellular telephones should receive the same protection from unlawful interception as do land-line telephone calls.

There are three areas that are of specific concern to the membership of the CCIA, and those are, one, that all calls involving cellular telephones must be protected against unlawful interception under 18 U.S.C. 2511; two, that data transmitted by cellular telephones must be similarly protected against interception; and, three, that the manufacture, possession, or sale of devices aimed at intercepting cellular or other telephone calls must be restricted under 18 U.S.C. 2512 in a manner that will effectively reduce opportunities for illegal interception.

That is basically a summary of our position, sir. We would be delighted to answer any questions and of course be of any further assistance to the committee or its staff that it would desire.

[The prepared statement of Mr. Schachman follows:]

Prepared Statement of Stephen Schachman

Mr. Chairman, and members of the Subcommittee, my name is Stephen Schachman. I am Vice President-External Affairs for Bell Atlantic Mobile Systems, Inc., which has been authorized by the Federal Communications Commission to provide cellular telephone service to certain cities in the mid-Atlantic region and is one of the two companies currently providing cellular telephone service in the Baltimore-Washington area. With me today is David Baum, Vice President of Metromedia Telecommunications, which is also authorized to provide cellular telephone service in the Baltimore-Washington area.

Mr. Baum and I are here today representing the Cellular Communications Industry Association (CCIA). CCIA is a national association of entities involved in the provision of cellular telephone service and technology, including 25 companies which operate cellular systems licensed or soon-to-be licensed by the Federal Communications Commission.

CCIA appreciates the opportunity to testify before this Subcommittee on the application to cellular telephone calls of the federal statute regarding unlawful interception of telephone calls.*/

It may be appropriate for me to give you a brief description of what cellular telephone service is. Cellular telephone is a new service that uses state-of-the-art technology -- small geographic cells and low power transmitters -- to provide mobile telephone service. Use of cellular technology results in substantial increases over traditional mobile telephone technology in the number of mobile telephone subscribers and the number of simultaneous mobile telephone calls that can be made in a particular area. Cellular telephone service is not available in over a dozen metropolitan areas in the United States and is expected to be available on a nationwide basis. Eventually, there may be millions of cellular telephone users.

---

*/ 18 U.S.C. § 2510 et seq.

Cellular telephone facilities can be used in three ways. A call may be made:

(1) from one cellular telephone to another cellular telephone, for example, car to car;

(2) from a cellular telephone to a landline telephone, for example, car to home; or

(3) from a landline telephone to a cellular telephone, for example, business office to car.

The only difference between these three types of calls is whether only radio frequencies are used (cellular to cellular calls) or whether telephone wires are also used (cellular to landline or landline to cellular calls). In all three of these cases, the parties to the call have the same expectation of protection from unlawful interception as they do with conventional landline telephone calls. Indeed, a recipient of a telephone call generally has no way of knowing whether the call he is getting is made from a cellular telephone or landline telephone. Similarly, the maker of a telephone call may not know whether he is calling a cellular telephone or a landline telephone, for example, when he is returning a message.

Given that cellular telephone calls and landline telephone calls are indistinguishable to users, cellular telephone calls should receive the same protection from unlawful interception as do landline telephone calls. I will outline three areas of concern in this regard.

(1) The federal unlawful interception statutes, 18 U.S.C. Sections 2510 through 2520, provides maximum protection to communications involving "wire communications,"*/ which include landline to landline telephone calls.**/ With regard to mobile telephone calls, however, as the Ninth Circuit has said, "[t]he definition of wire communication is not free from ambiguity."***/ Accordingly, the Ninth Circuit, over a decade ago, before the

---

*/ 18 U.S.C. §§ 2510, 2511.

**/ See U.S. v. Hall, 488 F.2d 193, 197 (9th Cir. 1973).

***/ Id., 488 F.2d at 196. Cf. U.S. v. Hoffa, 436 F.2d 1243 (7th Cir. 1970).

start of cellular telephone service, held that a telephone call from a mobile telephone to a landline telephone is protected by the statute, while a telephone call from a mobile telephone to another mobile telephone is not.*/ The court called its own decision "an absurd result," but found it to be required by statute.**/

CCIA agrees with the Ninth Circuit's characterization of its conclusion. It makes no sense to distinguish between the protection afforded to calls made from a telephone on the basis of what type of telephone the recipient of the call is using.

All cellular telephone calls should receive the same degree of statutory protection against unlawful interception as landline telephone calls. The expectation of protection from unlawful interception is the same for all telephone calls. What technology is used to complete particular calls is irrelevant. Accordingly, CCIA urges the Subcommittee to clarify any ambiguity in this area and confirm that all calls involving cellular telephones are protected by the provisions of Section 2511 of the statute.

(2) CCIA is also concerned that data transmitted via cellular telephone systems be similarly protected against interception. The transmission of data by cellular telephone technology will be expanding rapidly in the near future. For example, many banks currently have trucks that collect money and related data from branch offices and then, at the end of the day, transfer the funds and related information into central computers. In the future, such a bank truck could use cellular telephone technology to transfer the data to its central computer upon receipt, saving both time and money. Such uses of cellular telephone technology require strong protection against interception.

To the degree that cellular telephone data communications are covered by existing law, the Subcommittee should so specify. If legislation is needed, CCIA would be glad to work with the Subcommittee to develop it.

---

*/ Id., 488 F.2d at 197. State courts have also interpreted the statute in a restrictive manner. See State v. Howard, 35 Crim. L. Rep. (BNA) 2037 (Kan. 1984); Dorsey v. State, 402 So.2d 1178 (Fla. 1981).

**/ U.S. v. Hall, 488 F.2d at 197.

(3) Manufacture, possession or sale of devices aimed at intercepting cellular or other telephone calls should be restricted in a manner that will effectively reduce opportunities for illegal interception. Existing statutory restrictions*/ have been loosely interpreted to permit possession of devices that may have been built for illegal interception and are being used for illegal interception.**/ CCIA urges the Subcommittee to make it clear, through legislation if necessary, that manufacture, possession or sale of such interception devices is unlawful.

Mr. Chairman and members of the Subcommittee, on behalf of the Cellular Communications Industry Association, I again want to thank you for the opportunity to testify. The Association is ready to work with you and your staff.

I would be glad to answer any questions.

---

*/ 18 U.S.C. § 2512.

**/ U.S. v. Schweihs, 569 F.2d 965 (5th Cir. 1978).

Senator LEAHY. I find it somewhat fascinating the way the cellular industry is working. The interference people have had with mobile phones, for example; I had one small area of the State in Vermont where we have a mobile phone system. There is one or two channels and the inability to use it, the lack of channels, the inability to get on a line to use it.

And that I think probably built up in a lot of people's minds the awareness that this really was a radio transmission and somebody could pick up and listen in, especially if you have one of the really older style phones where you press channel by channel. You could listen in to anybody's conversation on that channel.

The cellular phone, with some variations, it is very much like using a phone that you are used to, the phone on your desk or something like that. You normally do not have to wait. You do not have something where again you can press in a channel and listen to somebody, or at least the typical car does not. So you start thinking of this as a regular phone. You start losing that kind of mindset, that this is something that somebody could be listening in.

Can the signal from these mobile phones be scrambled or encrypted and is that going to come about? Is the industry itself going to do something to make interception more difficult?

Mr. SCHACHMAN. Yes is the answer to your question. I think that the doctor from—it was formerly called Bell Labs. I am confused by all the names myself. There are a number of people working on

private encryption, but again it is the same thing that you discussed before, and that is the private party putting their own encryption device on. And what we get down to is a lot of people using this device who do not think in those terms necessarily.

And I am not sure that, say, in the banking industry which is looking very seriously at the ability to pick up from branch offices, from all these teller machines that we see, and instead of waiting until the end of the run 6 or 7 hours later, start transmitting that data from the back of a truck to its main computer banks, whether or not encryption is going to be something that is going to cause them to do that or not to do that.

And why should a party have to go to the expense of encryption where they do not necessarily have to do that in their own home.

Senator LEAHY. But you do not see a move within the industry just to automatically build encryption into each one of the cellular phones they sell?

Mr. SCHACHMAN. Not at this time, sir, no, I do not.

Senator LEAHY. We talked about the *Howard* case in Kansas, and there apparently the court went on the basis that there was ease of interception. Should the ease of interception be a factor in distinguishing among the different types of communication media?

Mr. SCHACHMAN. I certainly believe it should not be. I believe also that at this point in time there are not necessarily readily available although there are already discussions by manufacturers of devices that would ease the interception of cellular sometime in the future. And I believe that a clear signal from Congress that this is not what should be done may in fact impede the ease at which in the future cellular communications could be intercepted.

Senator LEAHY. When I was in law enforcement one of the banes of our existence was scanners that people could buy, and we found that in some cases it was the hobbyist sitting at home just kind of liking to hear where the police cars were going, and in my case whether the DA was calling home to find out if he was supposed to pick up anything at the grocery store.

But then we also found it was obviously a lot of criminals doing it, knowing where the patrol cars were, who was responding to an alarm system, and so on. Some of that we were able to get around with scrambling, but I was intrigued by the time I was leaving law enforcement how sophisticated it got, how it could scan all across and you could even program in for certain frequencies. If anything comes up on that it would home in in a microsecond.

Is it going to be possible to do similar monitoring systems for cellular phones?

Mr. SCHACHMAN. It is going to be more difficult to do it, but there are already people who are discussing and advertising the future advent of similar scanners.

Senator LEAHY. When the cellular system first started being talked about around here in Washington, there was a lot of discussion that there was really going to be an explosion of phones, and I suspect to some extent that will be limited by price.

But aside from the pricing aspect, from a technological stand, I have seen lobbyists walking around the halls of Congress with a little phone in their hand, and all people started talking about the shirt pocket phone. Is that a reality?

Mr. SCHACHMAN. I believe that it will be in a short time. One of the biggest drawbacks in reducing the size of the telephone is not the telephone side of the technology but the battery technology which has inhibited a lot of areas of technological growth. When that is overcome, right down to the Dick Tracy watch we'll be dealing with those. So you will never be able to get away from the telephone.

Senator LEAHY. Well, I think you have a terrible industry. [Laughter.]

Mr. SCHACHMAN. There are days when I would agree with you, sir.

Senator LEAHY. But, again, all that is going to be wire, at least on one end of it.

Mr. SCHACHMAN. One portion of it will be, and I think the important thing to note, that everything that was testified by the two gentlemen from AT&T, which is now done over traditional telephone systems, is probably going to be available in some mobile form, be it in your car or in your briefcase, in the not too distant future. And that is one of our concerns, the transmission of data, picture, facsimile, that will all be right there in your car or in your briefcase if you want it.

Senator LEAHY. Yes. And that I do not think anybody pays the least bit of attention to. The way things are going we have to be aware that that is coming.

Let me ask, Mr. Plesser, I look back at your report or at least a summary of the report of the Privacy Protection Study Commission. You were general counsel 10 years ago. I am concerned that little legislation followed. And yet a great deal of what you have got in that commission report is, if it did not anticipate the specific technology, certainly it anticipated the specific problem that we are faced with.

Let me ask you, I propose amending title III and you heard my statement out in Chicago to the ABA to include nonaural acquisition of the contents of a communication. Do you think if we took at least that modest first step that it is useful even though it is not addressing some of the more, some of the other privacy problems inherent in the new technology that has been discussed here today?

Mr. PLESSER. Absolutely. I mean, I think there is no question about that, and I think there may even be some vehicles in terms of looking at other bills that are going through Congress today in the computer crime area, that if one part of the problem is being resolved, it seems to me sensible to resolve the other problem.

And I really thank the Senator and the chairman of the subcommittee for having this hearing so late in the session, because I think it is one of those issues that really needs to be taken care of.

In the Privacy Commission report I think we were very sensitive of that technology, and so what we tried to do was create an institutional analysis. We did not care if it was a manual system, if it was a computer system. We wanted to know what the relationship between the individual and the institutions were. And as I think I said before, the only place I think we have fallen down is where there has been new institutions, where there are new people handling data that we did not conceive of before. I do not think the technology really should affect the rights, but if we have obvious

holes in the statute, like aural and digital, and the AT&T people saying, you know, that is not even a sensible distinction anymore because any particular telephone call could be half aural analog or digital. It is all mixed.

And so it seems to me there needs to be a clarification. I would say that one of the recommendations of the Privacy Commission was—and also we discussed at the ABA conference—was a need for continuing oversight of privacy technology issues, not only by congressional committees, which is being done, but by some entity in the Federal Government.

And I continue to think that that was probably the most significant recommendation of the Privacy Commission, and I think there is now some renewed interest in that coming from the ABA meeting that we were at. And I believe that that should be a high area of priority perhaps for next year.

Senator LEAHY. Those two areas, you mentioned the Congress and the executive branch, are they not really better suited to do this than the court? Are we not putting impossible burdens on the court to try to bring what I believe anyway is an outdated law to the realities of the latest technology?

Mr. PLESSER. I think I agree. I think the courts are not the right place now. I mean, I think they serve a role in enforcement, but no one is making policy. No one is looking at these issues in any long range—I have not seen any Federal papers on cellular technology, the privacy implications, that there has been anybody really seriously considering the implication of that one way or the other. Let them decide it one way, and at least it is a target to argue about, or electronic mail or packet switching or any of the other technologies.

And I think Congress should be in a position of telling the—would want to consider being in a position of telling the executive branch that they must consider this stuff. Even if I do not like what they come out with, it seems to me less important than somebody is looking at it.

What is frustrating to me as a privacy expert is not that the technology is advancing from the law, but what is frustrating to me now is that no one other than this committee and two or three committees on the House are really looking at these issues at all.

Everyone in the executive branch is just saying that it is going to go away. I do not think these issues are going to go away, and I think somebody needs to look at them.

Senator LEAHY. We have talked a lot about the involvement of laws with respect to governmental agencies, law enforcement agencies. But do you see Congress taking an active role in regulating private wiretaps?

Mr. PLESSER. Well, they have. I mean, title III regulates private wiretapping.

Senator LEAHY. It is an important thing for us to be looking at. Obviously, title III does not go anywhere near far enough in handling private wiretapping with today's technology. Do you see—a lot of the discussion in the past in this committee has been on the law enforcement aspects.

Mr. PLESSER. Oh, absolutely. I think that an individual should have an expectation of privacy, not only as to government entities,

but also as to private entities. And again I think one of the—the history of title III was that it was almost, I do not know, as concerned, but one of its principal concerns at that time was private intercepts, and its attempt was to put out of business this whole business of people who were making money intercepting for private interests. I think the idea of that statute was to put those people out.

Now the digital is not covered by the statute, as has been held by the fourth circuit in the *Seidlitz* case. I would think that the Safe Streets Act should be amended to knock out aural and make it clear that it covers all communications.

Senator LEAHY. That sort of deliciously vague "reasonable expectation of privacy," do you still see that, though, as being the basic standard to try to work in here?

Mr. PLESSER. I guess it is the only standard we have right at this point in time. I think it still is effective, but I think that it just cannot be taken care of by notice. In other words, if the people in Kansas, the judge in Kansas says, well, there is no expectation of privacy because they were told they were not going to have any, that does not seem to me to be a very satisfactory answer.

Senator LEAHY. Especially when you dial up one of these little chips, that every time you pick it up and you say hello and it goes "Beep: this is to alert you that you do not have a reasonable expectation of privacy." [Laughter.]

Mr. PLESSER. Little Brother.

Senator LEAHY. Little Brother. I like the standard. I just want to make sure that we do not, by retaining that standard, that we do not go the next step and say this covers this and then go into a technical description.

Mr. PLESSER. Let me just say that I like the standard, too, but I think there are some limitations with it. It is a standard. If we go back to FISA, there are no standards in FISA. There is no question—I mean, if there is an expectation of privacy, then they have to go through this process. But they do not have to make a demonstration once they are in the process in terms of how much, or how little, or is it justified.

And I think that the reliance on FISA is simply, you know, off the point, particularly in the application of the standard of expectation or fourth amendment protection or however you want to look at it.

Senator LEAHY. OK. I thank you all very, very much. We will stand in recess subject to the call of the Chair.

[Whereupon, at 11:53 a.m., the subcommittee was recessed, subject to the call of the Chair.]

○